HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

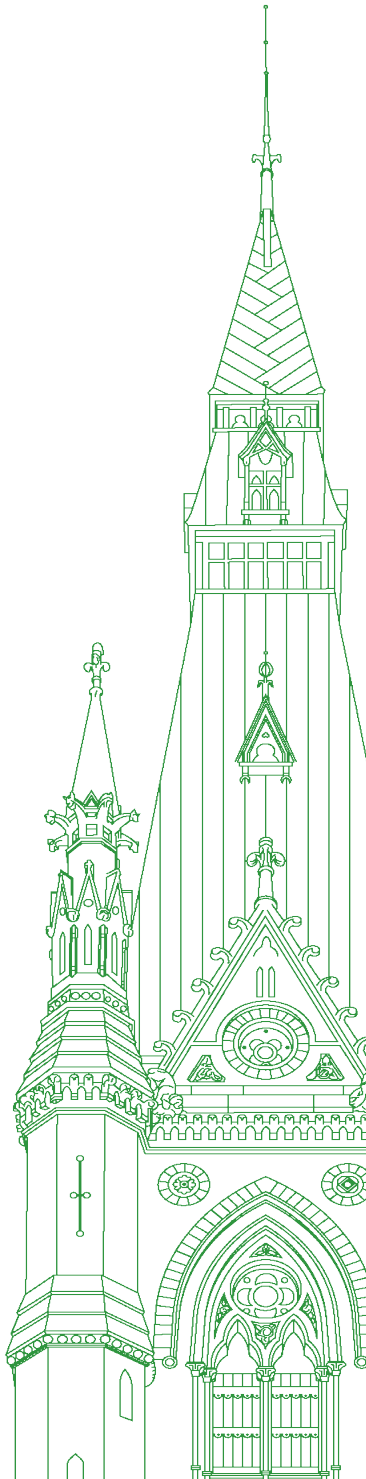
45th PARLIAMENT, 1st SESSION

Standing Committee on Public Safety and National Security

EVIDENCE

NUMBER 038

Tuesday, May 26, 2026



Chair: Jean-Yves Duclos

Standing Committee on Public Safety and National Security

Tuesday, May 26, 2026

● (1545)

[*Translation*]

The Chair (Hon. Jean-Yves Duclos (Québec Centre, Lib.)): Good morning, everyone. This meeting is called to order.

Welcome to meeting number 38 of the House of Commons Standing Committee on Public Safety and National Security.

If I may, I would like to move right away that we adopt the three budgets that the clerk sent last week. There was one for the study of the main estimates, a second for the study on the management of the Canada-United States border, and a third for the study of Bill C-22, which we are continuing today.

As you know, the amounts that have been provided to us are estimates. The committee could spend less than planned. Any unspent funds will be returned to the Liaison Committee.

If you have any questions, the clerk will be happy to answer them.

Is it the committee's pleasure to adopt the three budgets?

Some hon. members: Agreed.

We will now move on to the main topic of our meeting today.

Pursuant to the House of Commons order of reference of April 20, 2026, we are meeting today for consideration of Bill C-22, An Act Respecting Lawful Access.

Today we are fortunate to have with us many distinguished witnesses, whom I would like to welcome.

From the Barreau du Québec, we welcome Marcel-Olivier Nadeau, president of the Barreau du Québec, who is joining us by video conference; Nicolas Le Grand Alary, lawyer from the Secretariat of the Order and Legal Affairs, who is with us; and Michel Marchand, member of the Criminal Law Expert Group, who is joining us by video conference.

We also welcome Luc Lefebvre, chair and co-founder of Crypto Québec; as well as Philippe Dufresne and Marc Chénier, from the Offices of the Information and Privacy Commissioners of Canada.

I want to welcome each and every one of you back. You will each have the floor for five minutes for your presentations.

Mr. Marcel-Olivier Nadeau, you have the floor.

Marcel-Olivier Nadeau (President, Barreau du Québec): Thank you, Mr. Chair.

Members of the committee, thank you for having us here today.

Allow me to introduce myself. My name is Marcel-Olivier Nadeau, and I am the president of the Barreau du Québec. I am accompanied by Michel Marchand, a member of the Criminal Law Experts Group, and Nicolas Le Grand Alary, a lawyer with the Secretariat of the Order and Legal Affairs of the Barreau.

The Barreau du Québec thanks you for inviting us to take part in the consultations on Bill C-22. Let us recall that the mission of the Barreau du Québec is to protect the public, to promote accessible justice and to defend the rule of law. It is in that capacity that we are speaking today.

To begin, I would like to remind you of a fundamental principle. The concept of the rule of law is at the heart of our democracy. It requires that state powers be exercised, particularly in criminal investigations, within a framework, predictably and subject to independent judicial review. It also requires that laws uphold the fundamental rights guaranteed by the Canadian Charter of Rights and Freedoms, including the right to privacy and protection against unreasonable search and seizure. This balance is not theoretical. It is essential to maintaining public trust in our institutions.

The Barreau du Québec recognizes the legitimate objective of the bill, which is to modernize investigative tools in an ever-changing digital environment. We are nonetheless concerned about several provisions that could undermine fundamental rights, particularly when it comes to privacy and constitutional guarantees. Our goal is therefore to improve the bill so that it achieves its objectives without compromising the principles central to the rule of law or provoking court challenges.

Our recommendations focus on four main points.

First, the definition of subscriber information is too broad. The bill provides a very broad definition that is likely to reveal sensitive personal information when combined with other data, such as a person's name, alias, address, phone number and email address. The Supreme Court has also reminded us that the reasonable expectation of privacy must be analyzed in the current social and technological context, in which a massive quantity of data is collected, cross-referenced and retained. As a result, even isolated information can reveal a great deal when combined with other information.

Furthermore, the lack of a clear definition of the term “person providing services to the public” increases the risks of the invasion of privacy, as it allows for broad interpretation and potentially abusive applications. In the absence of legislative safeguards, this generic wording is likely to apply to a wide range of entities. That includes not only Internet service providers, but also companies and organizations with sensitive personal information.

This wording also creates uncertainty for the entities concerned, which could be forced to pass on sensitive information without clearly knowing whether they are legally required to do so. We recommend clarifying and narrowing these definitions to avoid overbreadth.

Second, the bill sets out an insufficient legal threshold for obtaining production orders. Under the bill, certain orders could be authorized on the basis of “reasonable grounds to suspect”, which is a lower threshold than is generally required for infringements of fundamental rights.

Let us not forget that the Supreme Court has established that subscriber information has a high level of constitutional protection, warranting rigorous judicial oversight. In our opinion, by stipulating the lower standard of mere suspicion, which does not require probability but only a reasonable possibility that an offence has been or will be committed, the bill does not meet constitutional privacy requirements. We therefore propose that, as with other similar orders currently in the Criminal Code, the threshold of “reasonable grounds to believe” be considered.

Third, there is a lack of judicial oversight in certain situations. Indeed, in certain cases, the bill allows for voluntary disclosure of information without judicial authorization, which we consider a significant departure from traditional safeguards in criminal law.

Let us not forget that even information that is considered “basic”, such as a subscriber's contact information or IP address, can, when linked to other elements, provide a detailed profile of the person in question. In this regard, the courts have found that it is imperative that the disclosure of this information be accompanied by procedural safeguards, including the requirement for prior judicial authorization. We recommend removing these mechanisms or, at the very least, requiring prior judicial oversight in all cases.

● (1550)

Fourth, the protection of solicitor-client privilege and computer data is at risk. The bill makes useful changes for the review of computer data. We maintain, however, that there should be a requirement that the extraction of computer data must be carried out by a person whose only role in the investigation of the offence in question is precisely to extract that data. That would be an effective way to avoid contamination of the investigation and, at the same time, to preserve solicitor-client privilege, which is a principle of fundamental justice as defined in the Canadian Charter of Rights and Freedoms.

The Chair: Mr. Nadeau, I'm going to have to ask you to speed things up.

Marcel-Olivier Nadeau: I'm done, Mr. Chair.

In conclusion, I would say that the Barreau du Québec invites legislators to review the bill in order to maintain a fair balance between the effectiveness of investigations and the protection of fundamental rights.

We look forward to your questions.

I'm sorry that I went a little bit over.

The Chair: I'm sorry to have interrupted you. If you wish, you will probably have an opportunity later on to elaborate on the last point you mentioned quickly.

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

Luc Lefebvre (Chairman and Co-founder, Crypto Québec): Mr. Chair, members of the committee, I appear before you today on behalf of Crypto Québec.

When I last appeared before this committee, as part of the consultations on Bill C-8, I concluded by saying that the Quebec model increased overall security by harmonizing security and privacy protections, and that the government should draw inspiration from this approach, which has already proven to be effective.

[*English*]

However, today we find ourselves faced with a bill that many information security professionals in the country and abroad, as well as several technology organizations, consider fairly dangerous. These are organizations whose applications are used daily by a very large number of elected Canadian officials as well as law enforcement. I am notably thinking of Signal from the Signal Foundation, which is threatening to leave the country if this bill is passed, so as not to weaken the encryption of its application.

In our opinion, this bill should be withdrawn and completely rethought. The basic premise of this bill is flawed.

[*Translation*]

Bill C-22 is based on a premise that has never been rigorously publicly demonstrated, which is that encryption is the main threat to public safety in Canada today. There is no evidence of that.

We've heard anecdotes from certain police forces and intelligence agencies, but we've never seen any empirical, public evidence that encryption is the greatest threat to Canada's national security.

On the contrary, it has been shown that the more data that is collected, the greater the risk of data leaks, without any real improvement in security.

[*English*]

To that effect, in the U.S., just a few years ago, it was demonstrated by The Washington Post that the FBI had massively overestimated the number of investigations allegedly blocked by encryption. These figures were then used publicly to justify the expansion of surveillance powers. We should not repeat the same mistake in Canada.

While we're being told about encryption being the problem, the actual public reports from the Canadian intelligence agencies, such as those from NSICOP, primarily tell us about foreign interference, deficient resources and the opaque expansion of the national security apparatus. The problem is thereby pretty clear. There's a lack of human, technical and financial resources as well as an excessive increase in data collection powers without any real oversight capacity. Bill C-22 addresses none of that.

[*Translation*]

Encryption is not the heart of this crisis; it is the solution.

Despite this, Bill C-22 proposes nothing less than the creation of a permanent digital monitoring infrastructure. It would be an infrastructure in which service providers could be forced to keep more data, maintain technical access capabilities, respond to secret orders, and participate in extraction processes, even though the word "oversight" appears exactly zero times in the text of the bill.

The bill also makes no specific reference to robust democratic checks and balances. This is extremely concerning. A healthy democracy is founded on privacy, freedom of association, confidentiality of communications, and spaces where citizens can discuss and criticize power without fear of permanent structural monitoring.

● (1555)

[*English*]

To Albertans and Quebeckers alike, I say this. No federal government should ever possess expanded structural surveillance capabilities in a context where major democratic and constitutional debates may one day oppose Ottawa and the provinces.

[*Translation*]

Canada's history reminds us that national security tools can sometimes extend beyond external threats and affect domestic political movements. That's precisely why stellar democratic guardrails are needed.

It is also important to note that if this bill passes in its current form, all the efforts made in terms of digital sovereignty in Quebec will become null and void.

[*English*]

Protecting democracy in Canada requires strong institutions that balance security and privacy with robust oversight, checks and balances. Bill C-22, unfortunately, gives the impression that the main threat to Canada is becoming increasingly internal rather than external. We all know this is a slippery slope for a liberal democracy.

In closing, we believe that the Canadian Parliament should not adopt such a fundamentally transformative bill based on unfounded assumptions, fears or premises that have not been publicly demonstrated. There is no back door that is only used by the good guys. The history of cybersecurity shows us precisely the opposite.

[*Translation*]

Since the likelihood of potential abuses and their effects are too great, we are calling for Bill C-22 to be withdrawn in its entirety.

Thank you.

The Chair: Thank you, Mr. Lefebvre.

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

Philippe Dufresne (Privacy Commissioner of Canada, Offices of the Information and Privacy Commissioners of Canada): Thank you, Mr. Chair.

Members of the committee, thank you for inviting me to share my views on Bill C-22.

Last week, I made a written submission to the committee, which I will address in greater detail today.

Bill C-22 reintroduces lawful access provisions that were originally proposed in Bill C-2, but with several changes that reflect feedback the government received. Some of these changes are consistent with written recommendations on Bill C-2 that I submitted to the Minister of Public Safety last November.

[*English*]

Bill C-22 improves on its predecessor, Bill C-2, in several respects. In particular, I welcome the more narrowly tailored confirmation of service demand. I appreciate the addition of potential privacy and cybersecurity impacts as factors that must be considered in the making of regulations and orders under the supporting authorized access to information act, the SAAIA. I'm also pleased to see the act's new oversight role for the intelligence commissioner with respect to ministerial orders.

That being said, in my written brief to this committee, I've highlighted some aspects of Bill C-22 that would warrant, in my view, further amendments to strengthen and ensure privacy protections for Canadians.

Specifically, I recommend narrowing the definition of "subscriber information" to a closed list of discrete identifiers, such as a subscriber's name, address, telephone number and IP address. This would help to avoid capturing information that could attract a heightened expectation of privacy.

I also recommend restricting the range of persons or entities who could be compelled to produce subscriber information to telecommunications service providers, and ensuring that the justice or judge making the order can specify the subscriber information that must be produced.

[*Translation*]

In addition, I recommend defining “publicly available information” to exclude information in respect of which an individual has a reasonable expectation of privacy, as defined in the Communications Security Establishment Act.

The concept of so-called publicly available information continues to evolve, and an individual does not automatically waive any reasonable expectation of privacy for information that may be available online. Take, for example, a situation where an individual's information was disclosed as a result of a data breach or published without their knowledge or consent.

[*English*]

Another recommended amendment would be to add an overarching requirement that obligations imposed under the SAAIA be limited to what is necessary and proportionate. This would help to ensure that any such obligations, including with respect to the retention of metadata, are tailored to minimize privacy impacts.

On the issue of accessing information, I would recommend amending the definition of “systemic vulnerability” to clarify that it includes any action that would render systemic methods of authentication or encryption less effective, as in Australia's analogous law. In addition, I recommend specifying that regulations and orders must not have the effect of requiring an electronic service provider to introduce, or of preventing an electronic service provider from rectifying, a systemic vulnerability.

● (1600)

[*Translation*]

Finally, I recommend adding an exemption to the confidentiality rules set out in the supporting Access to Information Act which would expressly authorize electronic service providers to share information with appropriate regulators, such as the Office of the Privacy Commissioner of Canada, to enable them to properly exercise their powers and duties.

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

The Chair: Thank you to all three of you for your presentations.

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

Frank Caputo (Kamloops—Thompson—Nicola, CPC): Thank you, Mr. Chair.

Thank you to our witnesses.

[*English*]

I'm going to start with Commissioner Dufresne. Thank you for being here again.

Can you please tell this committee how you were consulted on the drafting of this bill?

Philippe Dufresne: We were consulted by the Minister of Public Safety following Bill C-2. We made some recommendations to the minister. My staff met with staff from the minister's office. We had the opportunity to provide feedback. Some of it was taken up; some of it was not.

Frank Caputo: Am I correct in saying then that you, as the Privacy Commissioner, were not consulted on what should be in a bill that touches on so many people's online privacy?

Philippe Dufresne: As I said, we had an exchange. We were consulted post-Bill C-2 on what the next version should be. I would not say that we were not consulted in this instance. We made a number of recommendations. A number of them were taken and I've highlighted those improvements, but there remain many that were not: necessity and proportionality, safeguarding, the narrowing of the definition....

There remain privacy concerns, hence my submission to this committee.

Frank Caputo: I'm not sure if you've been watching this committee process, Commissioner Dufresne. One of the chief issues I have here is how quickly we are moving.

How many eminent witnesses do we have here? We have six very qualified witnesses representing three parties. This really should be divided up into two panels, in my view. I won't get to ask half the questions.

Can you comment? Does it feel to you like this has been a bit too rushed? You gave us five or six substantive amendments here. We're not even going to be able to ask you about a lot of them because we're quite short on time, without even getting to other valid points. From your observation, has this been rushed?

Philippe Dufresne: The committee is the master of its proceedings, but I did send a written brief last week, knowing that there was less time. We've made attempts to make it user-friendly and clear as to what our expectations are. We have eight specific recommendations to improve the bill from a privacy standpoint.

Frank Caputo: I'm mindful of that. I know you really can't weigh in.

Mr. Lefebvre, you have been observing this. Does this not feel rushed to you? It feels quite rushed to me.

Luc Lefebvre: Absolutely, it feels pretty rushed, particularly knowing that this is a bill that has an impact on every Canadian.

You know what they say. With extraordinary power comes extraordinary responsibility. I have the impression that they are asking for extraordinary power, but we don't know why. It seems that it has not been profoundly thought through, because it has many implications for everyone. We understand that this comes from a place of need and requirements from law enforcement and our intelligence agencies, but the impacts are so great that it needs to be discussed further.

Frank Caputo: I would agree with you. No one is doubting that we want to catch bad people, like terrorists, and—as in my prior life—catch people who abuse kids. There's no doubt about it.

You also hit the nail on the head. Not only has this been rushed, but the communications from the government have been awful, if I'm going to be candid about this. The minister would not declare whether he would be open to an amendment on encryption, which is something that you highlighted. I don't know why we're using cute phrases like “encryption-neutral”. We don't know any of that.

Amendments have to be in tomorrow, yet we're hearing from officials on Thursday. We've had one hour from officials. From your standpoint, can you see why it would be prudent to actually study this bill further?

● (1605)

Luc Lefebvre: Like I said before, the implications are grand. Every country that went that way, because there are other countries in the Five Eyes that went that way.... When I think of Australia and the United Kingdom, they took the time to think about it. They went a different way from what I wish they would have gone, but they took more time.

This matter affects businesses. It affects every citizen, and it affects every part of everyday life. It needs to be more thought through.

Frank Caputo: I understand.

I'm sorry, but I have to cut my time short with you because I'm down to about 45 seconds.

Mr. Nadeau, one of the things you talked about was oversight and people getting caught. Right now, the intelligence commissioner has to approve or sign off on a ministerial order. What would you say to an amendment that would require judicial oversight? In other words, rather than the intelligence commissioner, having the Federal Court of Canada.... Rather than having to go through judicial review as an extra step, it would go to the Federal Court of Canada in order to approve a ministerial order.

[*Translation*]

Marcel-Olivier Nadeau: Thank you for your question, sir.

I will let our expert, Mr. Marchand, answer.

Michel Marchand (Member, Criminal Law Expert Group, Barreau du Québec): Hello.

That's a broad question and one that is difficult to answer. We'll have to see what the content of the ministerial order is. It's hard to answer the question without knowing all the parameters.

The Chair: Thank you for that brief answer.

In any case, we've gone over the six minutes allotted for this round.

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

Sima Acan (Oakville West, Lib.): Thank you, Mr. Chair.

[*English*]

Monsieur Dufresne, the scope of this legislation is to provide basic information on an individual, not the content of their data, not what they browse and not what is in their emails. The department has taken the time to carefully consider privacy concerns and charter considerations. However, we have heard concerns that the current wording in proposed section 487.011 could capture services outside Internet service providers, worded as “who provides services to the public”.

As the Privacy Commissioner, what language changes would you suggest to narrow the scope of services captured in proposed section 487.011 so that these concerns are addressed, while ensuring law enforcement have tools to access the information they need?

Philippe Dufresne: Absolutely, it's important that this bill balance the need for police forces to have the tools they need with protecting Canadians' privacy, and we can do that. It's not a zero-sum game between privacy and security. We address this in our written brief in our first three recommendations.

Specifically, the first thing that should be done is to narrow the definition of “subscriber information”. Change it from what it is here, which includes broader concepts like “information that may be used to identify” individuals or “information relating to the services”, and narrow that to specific items such as the name, address, telephone number and email address. We specify that in our brief.

The second thing is to restrict the scope of who can get those orders to telecommunications service providers. That's already there for the warrantless requests on confirmation of service demand, but in terms of the subscriber information, it's open to “a person who provides services”. That in our view is too broad. It could capture medical offices and law offices, and capture any amount of sensitive information.

The last element is that you should provide more specificity in terms of what the judge's order will be. Right now, it says “any subscriber information” and “all the subscriber information” related to something, and that could be broad. We're suggesting a narrowing of that language.

I'll flag the last element in terms of the non-warrant search or confirmation of service demand. There's an exception for medical and privileged information, and that exception is also absent in terms of the subscriber information.

Those are the recommendations I would make.

Sima Acan: Thank you very much, Mr. Dufresne.

To continue, we also had the privilege of hearing from the National Security and Intelligence Review Agency and the intelligence commissioner, who holds our national security regime accountable. In contrast, as the Privacy Commissioner, you play an important role to ensure federal departments and agencies adhere to personal information-handling practices.

What would you recommend to be added in relation to ministerial orders that will take this legislation to the next step?

● (1610)

Philippe Dufresne: I welcome the addition of the intelligence commissioner review role. That is an important improvement that was made, and I fully support it. I think the addition of necessity and proportionality to the scope of orders that could be made by the Governor in Council and by the minister is critical. That's a concept in privacy law that's shared around the world. In fact, the signatories to the OECD's December 2022 declaration on government access to private sector information unanimously and expressly called for “necessity” and “proportionality”. It's very important.

I believe Intelligence Commissioner Noël also talked about the notion of reasonableness and proportionality. That is a very important standard. There's some language in the legislation that calls for a consideration of privacy impacts. That's a good thing, but it needs to go further, in my view, to be necessary and proportional.

Sima Acan: Thank you, Mr. Dufresne.

Monsieur Nadeau, from my understanding, you would like a tighter definition of “subscriber information”. Currently in part 1 of the bill, a confirmation of service demand asks a simple yes-or-no question to determine if an individual uses the service. In addition, the definition of “subscriber information” in proposed section 487.011 focuses on identifiers—in other words, basic information. It's not the content of the data, such as what you browse or what's in your email.

Could you explain what you would like to see added to proposed section 487.011 to narrow the definition and the scope?

[*Translation*]

Marcel-Olivier Nadeau: Thank you for your question.

I think the commissioner gave some great examples just now. I don't have any more to add, but I will let Mr. Marchand or Mr. Le Grand Alary provide you with other examples, if they have any. The ones that were just given by the Privacy Commissioner are excellent, and I would adopt them, as well as the principles he set out.

[*English*]

Sima Acan: Thank you very much.

[*Translation*]

Nicolas Le Grand Alary (Lawyer, Secretariat of the Order and Legal Affairs, Barreau du Québec): Thank you, Mr. Nadeau.

I was actually going to add one point. I think the commissioner did a good job of explaining the concerns. There's the concept of subscriber information and also the court order. All of these elements are problematic; it's the whole thing. The three definitions need to be tightened up. I think the commissioner did a good job of explaining the issue.

[*English*]

Sima Acan: Thank you very much, Mr. Chair.

My time is up.

[*Translation*]

The Chair: Thank you very much, Ms. Acan.

Mr. Lloyd, please go ahead for six minutes.

I'm sorry, it's your turn, Mrs. DeBellefeuille. My humble apologies. It's impossible to forget you, but I still managed to do so.

You have the floor for six minutes.

Claude DeBellefeuille (Beauharnois—Salaberry—Soulanges—Huntingdon, BQ): Thank you, Mr. Chair.

Let me start by saying how disappointed I am to have so little speaking time with such a rich panel of witnesses.

Since time is limited, I will try to keep my questions short, so you can provide clear answers.

Personally, the more I learn, the more confused I am. The views on the bill are vastly divergent and very polarized, depending on whether we're speaking to a police officer or a privacy advocate. My goal is to tell stakeholders that, yes, this is an important and necessary bill, but also to figure out what that balance is going to look like.

Mr. Dufresne, I'm always surprised that your recommendations aren't heeded before a bill is drafted. We're always a bit behind. We went through that with Bill C-8. No one bothered to consult you. Now you're here with your recommendations, and opposition parties are the ones proposing them as amendments to the bill. I find that strange, especially since we have so little time to debate them. We would have preferred that the government do its job, listen to you and include your seemingly reasonable recommendations in the bill. It would have made for a better bill and saved us time.

Mr. Lefebvre, you got my attention when you said a lawful access regime had not been shown to lead to a decrease in crime in the U.S. There is no evidence of that. Weaker encryption doesn't necessarily equal less crime. Here's what police tell us: They'll be more effective, they'll stop more criminals and they'll be able to combat organized crime.

You seem to be telling us it's not that straightforward.

Can you give us more information on that?

● (1615)

Luc Lefebvre: The tendency to try to control what we call lawful access in Five Eyes countries goes back 10 or 15 years. Australia's and the United Kingdom's laws are particularly robust when it comes to collecting data for the stated purpose of combatting pedocriminality, going after criminals and such.

To date, however, there is no evidence that crime decreases when law enforcement has greater access and more say over the level of encryption of applications, messaging platforms and other tools. Those broader powers have not been shown to lead to a decrease. At the end of the day, more information is being collected, but crime isn't going down. That's all this is doing.

What we actually see with the broadening of powers is that criminals tend to go dark. They use other methods, other tools, and the trail ends up going cold anyway. Nevertheless, more and more data are being collected on ordinary people—people who aren't involved in these activities.

Claude DeBellefeuille: Let's look at models we want to draw on, the U.K.'s, for instance, or New Zealand's or Australia's. The U.K. even installed cameras that record citizens as they go about their everyday lives. It's taken surveillance to the extreme.

Has it been shown to bring the crime rate down?

Luc Lefebvre: That correlation hasn't been made. The U.K. is known for its widespread use of closed-circuit TV, or CCTV, monitoring. In addition, the U.K. has passed very robust laws on data collection and freedom of expression. A correlation between that and a significant reduction in crime hasn't been shown, but that was the official excuse that was given.

Claude DeBellefeuille: I attended an event put on by the Canadian Association of Chiefs of Police, and there was a lot of excitement in that room. People said they'd been waiting 30 years for legislation like this.

Why do you think the government is in such a rush to pass this bill? Are there any countries pushing us in that direction?

Luc Lefebvre: I would say two things to that.

First, it makes sense that police services would welcome this legislation. I come from a family of police officers who were involved in fighting pedocriminality and the like. I completely understand the excitement, and it's necessary. It's no surprise that police forces are pleased about this. It's perfectly commendable.

Second, my sense is that the pressure is coming mainly from members of the Five Eyes group, which is looking for more and more visibility across the network, as well as from allies. Canada is indeed lagging behind when it comes to being able to provide access to those data. There's clearly some political pressure to do that.

It's probably the easiest solution for the government to say that it's going to bypass encryption to give police forces access to Canadians' data. Police will be happy. It's easier than allocating more financial, technical and human resources to fighting crime. At the same time, it will make our allies happy. That's the impression I have.

Claude DeBellefeuille: Mr. Dufresne, as you know, the deadline for us to submit our amendments is 5 p.m. tomorrow.

Are your recommendations already in amendment form, so we can use them and submit them as is?

Philippe Dufresne: They aren't drafted how the Office of the Law Clerk would draft them, but I don't think it should be too difficult to turn them into amendments, given how we've laid them out in our brief.

We refer to existing regimes, such as Australia's law, which stipulates that orders must not have the effect of rendering encryption less effective. That amendment is in there. One of the provisions in the bill we're concerned about says that the provider is not required to comply with an order.

We feel it's important to state that the order shouldn't be made at all. It puts the provider in a tough spot. They are being ordered to do something but are allowed to disobey the order under the law. I think things should be done right from the start.

We addressed necessity and proportionality, referring to Great Britain, which takes those factors into account. Australia does too. They are core principles, so it's not hard. They can be added to the factors the minister or Governor in Council has to take into account.

The eight recommendations we've made are targeted and concise. Essentially, they're intended to achieve that critical balance.

● (1620)

Claude DeBellefeuille: Thank you very much, gentlemen.

The Chair: Thank you, Mrs. DeBellefeuille.

[*English*]

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

The Chair: Go ahead, MP Lloyd.

Dane Lloyd: Thank you, Mr. Chair. I wanted to wait until my colleague Madame DeBellefeuille was finished.

I heard the Privacy Commissioner tell us about a submission he made to this committee. I believe the submission was sent to the chair on May 21. We had not received that submission until just now.

I'm not trying to attribute malice to anyone, but my ability, as a parliamentarian, to scrutinize this legislation and be prepared for today's meeting was really impacted. By not receiving documents sent in by witnesses, I have no ability to properly review them.

As an aside on another point, we still don't have the transcript from our meeting two weeks ago. I just raised this with our clerk, who assures me that it's coming. You know, we had a two-week break. If we're not able to get critical information to help us do this, given the rushed nature of this legislation we're sending through.... I have very serious reservations about how quickly this process is going, as we're not being given adequate information and evidence to get this bill done.

The Chair: Thank you. That is not exactly a point of order. It's more like a point of privilege, but I think we understand the value of it.

The clerk just informed me a couple of minutes ago that for reasons that are human, he wasn't able to send it earlier. He wants to express his discomfort with that. Now he has received it, so I encourage everyone to look at your emails. The full document was just shared.

On the transcript, maybe I should know a bit more about what the clerk has to provide as a matter of precision.

Mr. Clerk.

The Clerk of the Committee (Paul Cardegna): Thank you, Mr. Chair.

With regard to the transcript, we have been informed that the publications department of the House of Commons has set service standards. I can look into those service standards and get back to the committee, as I don't have them with me right now. However, they wrote to me on Friday indicating that there have been some delays, notwithstanding the length of the meeting on May 7, which was four hours instead of two, and the large volume coming through their office as well. They've indicated that they are working as hard as they can to get that transcript out.

I can send the blues to you right now, Mr. Lloyd, and I will do that. The blues are usually available within the firewall. If any member cannot access them, we can send copies to them.

With regard to the document from the Privacy Commissioner, that mistake was entirely mine. I do apologize to the committee. Unfortunately, it slipped through my fingers and I did not get it out in as timely a fashion as I would have preferred. I beg the committee's indulgence on that. You have my apologies.

Thank you.

The Chair: MP Lloyd, go ahead, and then we'll go to to MP Caputo.

Dane Lloyd: Maybe I'll cede the floor to Mr. Caputo.

Frank Caputo: Chair, I'm fine with MP Lloyd going first. He has a train of thought.

Dane Lloyd: Thank you.

I really do appreciate the explanation from the clerk. We know that accidents like this happen.

I was told that we could access the blues within the firewall on our devices. I have my House of Commons phone here. I just looked, and the blues are not available on my House of Commons phone.

You know, despite the fact that this does look like it was an honest mistake, given the gravity of the legislation we have before us, I feel that I've been really disadvantaged and that my privilege has been violated by not being able to have the correct information available to me in order to participate in the session. I'm looking for some guidance from the chair. I believe my privilege has been violated here.

The Chair: Thank you. I'll take that into consideration and work with the clerk—not now but immediately after this meeting—to see, with everyone else's input, what we can do to facilitate the important work that needs to be done in such a short amount of time.

Everyone, please note that you now have the document shared earlier by the commissioner. We can use that with our teams to move forward.

Again, I'll come back to this aspect of the breach of privilege, which you correctly stated.

Having said that, MP Caputo, would you like to say something before we turn to MP Lloyd for his five minutes?

● (1625)

Frank Caputo: Yes. I'll intervene just briefly.

Given what Mr. Lloyd has reflected on, that his privilege has been breached, and not even as a prima facie breach but as an obvious breach, I would ask, Mr. Chair, if you and the clerk would be able to canvass the Privacy Commissioner's ability to return next week and, in any event, prior to clause-by-clause consideration.

I also think the appropriate remedy here is that we do not have amendments close tomorrow. I think it's very obvious that this is the only remedy in what is already a very rushed process. I think this is symptomatic of the fact that we have been moving very quickly. I do not place any blame on the clerk. These things happen. Mistakes happen. We've had four-hour meetings. We're in the midst of another four-hour meeting.

I won't say any more. Thank you.

The Chair: On that, first, we have important work to do now, so I suggest we do it now. Second, as I said, I will review the matter of the breach of privilege raised by MP Lloyd, and third, thereafter, we will work together—I'll work with you in particular, MP Caputo—to see how the suggestion of changing the schedule for consideration of this bill may be accepted by other members of the committee.

Frank Caputo: I am concerned, actually, Mr. Chair. This is something I'm thinking about contemporaneously here. Does a question of privilege not need to be dealt with now, at the first possible instance? I would ask that you please consult with the clerk if we need to suspend. It is important that we get this done right, not that we get this done quickly.

The Chair: Questions of privilege don't have to be decided now by the chair. I can ask for the indulgence of the committee to reflect on that—with the assistance of the clerk, obviously, and others—after the meeting to see how we proceed there. If it were a point of order, it would be different. This is a question of privilege, and I can take it into consideration after this meeting.

I would advise the committee that we do this and take advantage of the witnesses who are now present to push forward the analysis of the bill under consideration.

Having said that, would you like to start your five-minute intervention, MP Lloyd?

Dane Lloyd: Just as soon as I.... Oh, I'm sorry.

[*Translation*]

The Chair: Go ahead, Mrs. DeBellefeuille.

Claude DeBellefeuille: Mr. Chair, I want to echo the important point Mr. Lloyd made. I was waiting for that brief to prepare amendments. I'm always shocked at the fact that the Privacy Commissioner of Canada's recommendations are never taken into account before measures are drafted. I was eagerly waiting for the brief, because I knew what a tight deadline we had.

I think the point of privilege is relevant. I think it's really important to look at how you're going to proceed. We want to feel that we're able to submit those recommendations and that the commissioner's comments have been taken into account.

The Chair: As I said a moment ago, I will consider the matter. The information should have been available a while ago. It's available now. It's a four-page document. As the commissioner himself said, the recommendations are well laid out. They are clear and should be fairly easy for committee members to understand.

That said, I suggest we resume the discussion with the witnesses we have today. I can give you the various experts' opinions and recommendations, including the clerk's, after the meeting.

I hope that's okay with you, Mr. Lloyd. We need to keep going. Otherwise, things will have wait until the next meeting.

[*English*]

Dane Lloyd: Thank you to the witnesses.

Commissioner Dufresne, we had another witness here today who said that he believes the reasonable suspicion threshold for subscriber data is too low. Do you have thoughts on that, or is that outside your scope?

Philippe Dufresne: I would think it's too low with the current framing of the scope of subscriber information: the definition and the parties that can receive it. My recommendation is to fix the scope. If you fix the scope, I think you can keep the suspicion, but if you don't, that would be the alternative.

Dane Lloyd: Okay. Thank you for that. You're giving us multiple options here.

What are your thoughts about the non-disclosure rules? If an authority goes to an electronic service provider for a subscriber request, they can place a non-disclosure so that the provider can't tell the subject of that request that there's been a disclosure. What are your thoughts on that?

● (1630)

Philippe Dufresne: There could be some valid reasons for that confidentiality. There are improvements in the bill in terms of reports from the minister to Parliament and so on.

One of the gaps I'm identifying in my eight recommendations is that the confidentiality would prevent the provider from notifying my office if there's a breach and if there's relevant information in a ministerial order. That is, in my view, a gap that should be addressed, because it prevents us from doing our work.

Dane Lloyd: Would it be fair to say that your recommendation is that any time an authority asks for subscriber information your office be notified?

Philippe Dufresne: Not necessarily, but I would not want to have the confidentiality provision prevent sharing of information where it's appropriate: with my office, for instance, in a privacy breach. That's the most obvious situation.

When we're dealing with this issue of subscriber information and the encryption, the safeguarding of information is absolutely key.

Dane Lloyd: Yes. I think there are cases where non-disclosure is absolutely necessary: for example, active investigations. Do you think adding judicial authorization when seeking a non-disclosure order would be an appropriate way to strengthen?

Philippe Dufresne: It strengthens it from a privacy standpoint. You would have to weigh that with the impact on the police work. This is not one of my priority eight recommendations that I've made, but it's a consideration.

Dane Lloyd: It's a trade-off.

Philippe Dufresne: I suspect it would create some delays.

Dane Lloyd: Okay. Thank you.

Now, about metadata, there's been a lot of talk about a requirement to hold metadata for a year. You talked about “necessary and proportional”. Is it necessary and proportional to hold the metadata of all Canadians for up to a year?

Philippe Dufresne: I think that condition of necessity and proportionality has to be there whenever you exercise that power, whether it's cabinet in terms of the orders or whether it's the minister. With that framing, you're going to deal with it on a case-by-case situation. There may be situations where it's so severe and it's so significant that there may be some reasons. That would be for the government to provide that or for the police to provide that. I don't want to prejudge it. Without that framing, then, you risk having the orders being too long and too broad. This is why necessity and proportionality are such a key part of privacy law.

Dane Lloyd: Are you concerned about the privacy implications of companies being mandated to hold on to Canadians' metadata for a year?

Philippe Dufresne: The longer you keep information, the more there's a risk in terms of a privacy breach and the more there is an impact if there's a privacy breach. One of the principles we put forward is to not retain information longer than is necessary. Again, that's why necessity and proportionality are so important. There will be cases where you need to keep it longer, but that should be tested in every case.

Dane Lloyd: We've heard of systemic vulnerability. The government has said that it will not introduce systemic vulnerabilities. However, it looks like, under the ministerial orders, it could very well order companies to install things that could create vulnerabilities.

What are your thoughts on that?

Philippe Dufresne: I know that there have been debates on this. The bill now has a definition of "systemic vulnerability". I think I heard government officials say that it is not their intention to diminish this.

What I'm proposing is to make that clear in the legislation. We have a model for that in Australia, where it—

Dane Lloyd: I'm sorry.

With my final bit of time, Mr. Lefebvre, I heard from a constituent who came to my office last week. He's concerned that if we create potential back doors, which could definitely be done under this legislation—maybe not right away—damaging information about people could be fabricated and added to their accounts to make them look like they're guilty.

Is this a tactic that extortionists use? Could they exploit encryption breakthroughs to do this?

Luc Lefebvre: If there's a back door, it can basically be used by anybody, even the people who are not supposed to use it.

Obviously, once you have access to data, you can manipulate it in any way. It's obviously something that I would say bad actors, criminals or adversaries could use to fabricate some claim about somebody.

[*Translation*]

The Chair: Thank you, Mr. Lloyd.

We now go to Mr. Ramsay for five minutes.

Jacques Ramsay (La Prairie—Atateken, Lib.): Mr. Lefebvre, are metadata encrypted?

Luc Lefebvre: It depends. Some—

Jacques Ramsay: I don't think so.

Luc Lefebvre: Actually, some metadata are encrypted, depending on the system. Signal is a great example.

On Signal, the metadata are encrypted. Data that aren't encrypted include the account creation date and the last date of a user's connectivity. However, once a user is connected to Signal and in their account, there's no way to know who a user is communicating with, when or what the content of their discussions is, as opposed to email.

With an email application, certain data are available: who communicated with who and when, what server the email was sent on, what the subject of the email was. The content of the message isn't necessarily available, but those metadata are. It all depends on the type of system, on the type of encryption the application uses.

In this case, the purpose is to access data that weren't previously available, such as in Signal, by reducing the level of encryption.

● (1635)

Jacques Ramsay: Okay. I accept your definition, Mr. Lefebvre. Signal stands out because of the secrecy around its metadata.

Unless I'm mistaken, messages are encrypted most of the time, and the government made clear that it didn't want any information in the messages. We are talking about dates, locations and other such data. That isn't encrypted information. The government isn't on a mission to decrypt people's communications.

Mr. Dufresne, you say that the government is there to go after the bad guys. We aren't there to look at information about people's health. We aren't there for that.

Given that we and our colleagues opposite didn't see your report, can you tell us your main recommendation to ensure that the legislation captures only information relating to criminal activity?

Philippe Dufresne: I would say recommendations 1, 2 and 3 in the brief.

The purpose is to limit the type of information that can be obtained. I think that's what the government is trying to do, so specifying the information in question will reassure those who are concerned.

The idea is also to limit the types of persons and entities subject to these orders. As it stands, the production order applies to any person who provides services to the public. That's a broad range of people, so it would be possible to obtain people's medical information, for instance.

I think it should be limited to telecommunications service providers, as in the earlier provisions relating to non-warrant requests. I think that would restrict access to only the information the bill is really trying to capture.

Jacques Ramsay: All right. Thank you.

Now I'd like the Quebec bar association representatives to help me out. I'm not a lawyer, but the lawyers you represent include prosecutors.

Isn't that right?

Marcel-Olivier Nadeau: I wouldn't say we represent them, Mr. Ramsay, but they are indeed members.

Jacques Ramsay: They have to be, since they pay dues.

Marcel-Olivier Nadeau: Absolutely.

Jacques Ramsay: Did you consult them when you were preparing your brief?

Marcel-Olivier Nadeau: Yes.

We consulted a panel of criminal law experts. Half the members are criminal lawyers, and the other half are prosecutors.

Jacques Ramsay: All right.

You talked about the threshold and the difference between “reasonable grounds to suspect” and “reasonable grounds to believe”.

Obviously, no one is against virtue. Everyone would prefer a higher threshold. The premise of the government, however, is that the information being sought, in other words, metadata, isn't evidence that can be presented to the court. It's information that will help further an investigation, to obtain evidence that can ultimately be used in court. That is why the government used the “reasonable grounds to suspect” threshold instead of “reasonable grounds to believe”. It is an accepted, recognized and well-known legal standard, after all.

Marcel-Olivier Nadeau: I'm going to let Mr. Marchand speak to that.

Michel Marchand: In our view, suspicion is too low of a threshold. In Bykovets, the Supreme Court points out how much providing access to an individual's IP address violates their privacy. Obtaining an IP address provides access to everything.

The way the bill is currently worded, with reasonable grounds to suspect as the threshold for a confirmation-of-service demand, the purpose is merely to obtain information that will assist in the investigation. The reason for the demand is not that the suspect may have committed an offence. It's that the information will assist in the investigation.

The authoritative decision on reasonable suspicion establishes that this standard captures a lot of people who are not involved.

It was therefore—

● (1640)

Jacques Ramsay: The second condition is precisely why the information will assist in the investigation and—

The Chair: Sorry to cut you off—

Jacques Ramsay: I don't agree with you that this provides access to everything. That's not true.

The Chair: Sorry to cut you off, Mr. Ramsay, but we have to move on to Mrs.—

[*English*]

Frank Caputo: I have a point of order, please.

For a moment there, I thought it was me and the minister with Mr. Ramsay and our witness, but my point of order has to do with Mr. Lloyd's issue of privilege.

I've spoken with the clerk. I would ask that the clerk confirm on the record and that you, Mr. Chair, confirm on the record that you did not see the submission from the Privacy Commissioner, and that the clerk, to the best of his knowledge, did not forward it to you.

Is it accurate, Mr. Chair, that you did not see the submission from the Privacy Commissioner?

The Chair: I appreciate your question, MP Caputo. As I said earlier, this matter of privilege deserves appropriate attention. My attention now is focused on having the witnesses provide the most from their time and their input. If you allow, I will look at this after the meeting and consider this question of privilege in the appropriate manner.

Frank Caputo: With the greatest of respect, Mr. Chair, we have to decide how we are going to proceed.

If you did not receive this or did receive this, that does impact things. All I'm asking of you, Mr. Chair, is for a yes or no on whether you had seen the submission from the Privacy Commissioner.

The Chair: My understanding is that I did not see this email, but I want to double-check that and be certain that I provide the members of this committee with the most accurate information.

Frank Caputo: Thank you.

The Chair: Having said that, we'll go to Madame DeBellefeuille.

[*Translation*]

Mrs. DeBellefeuille, you may go ahead for two and a half minutes.

Claude DeBellefeuille: Thank you, Mr. Chair.

Mr. Nadeau, my questions are along the same lines as the parliamentary secretary's, so I'm going to continue the discussion with Mr. Marchand.

Basically, if I understand correctly, the “reasonable grounds to suspect” threshold in Bill C-22 applies to specific data that aren't considered sensitive.

You are arguing the opposite. The Minister of Justice, the justice department and department officials are saying this respects the Supreme Court's decision, but you don't seem to agree.

Can you elaborate on why you think that, to help us really understand your point?

Michel Marchand: We don't think it respects the Supreme Court's decision at all. Proposed new section 487.0142 of the Criminal Code is very broad, referring to “all the subscriber information…including transmission data”. That can all be captured through the IP address. Furthermore, if you read the Supreme Court's decision in Bykovets—which isn't that old—properly and carefully, you see that the majority of the court viewed the IP address as a gateway.

Search and seizure doesn't work the same way anymore. Before, when police officers did a search, they showed up at the individual's home and either they found something or they didn't. Now, with the IP address, they can access just about anything about the person, medical records, what they dream about, what they post online and all kinds of other information. On top of that, the bill says that the information can be retained for a year, which is like giving authorities access to a huge data bank they can use to spy on people or find whatever information they want.

Claude DeBellefeuille: Thank you, Mr. Marchand. I think I understand your point now. You're part of an expert group at the Quebec bar association. If a skeptical person shared that view with us, we might not believe them, but you're a very credible source, as far as I'm concerned.

I'm trying to figure out how we can make the bill better. You're recommending that we remove the “reasonable grounds to suspect” threshold.

The commissioner recommends limiting its use.

That's what I understood from your recommendations, Mr. Dufresne.

Philippe Dufresne: Exactly. You have both options.

Claude DeBellefeuille: To wrap up, I'd like to thank you.

The Chair: Mrs. DeBellefeuille, you're out of time, so I have to stop you there, I'm afraid.

Claude DeBellefeuille: Thank you.

You see how polite he is with me.

The Chair: It saddens me to hear you say such harsh words.

I thank all the witnesses for taking the time to prepare for the meeting and for travelling here or participating via video conference.

We won't have much opportunity to bid you a warm farewell after you leave, because we must begin the second part of the meeting. So, we invite you to have a good rest of your day. Thank you.

● (1645)

(Pause)

● (1649)

● (1645)

The Chair: Good morning, everyone.

We are beginning the second part of this meeting with new witnesses, whom I would like to welcome.

We are joined by Erik Neuenschwander, senior director of User Privacy and Child Safety, from Apple.

From the Canadian Civil Liberties Association, we are joined by Tamir Israel, director of the Privacy, Surveillance, and Technology Program. He is participating in the meeting via video conference.

From Google, we have Katherine Charlet, senior director, and Jeanette Patell, director of Government Affairs and Public Policy, both participating via video conference.

We will now begin the five-minute presentations.

Mr. Neuenschwander, you have the floor.

● (1650)

[*English*]

Erik Neuenschwander (Senior Director, User Privacy and Child Safety, Apple Inc.): Thank you.

Good afternoon, Mr. Chair, vice-chairs and members of the committee. My name is Erik Neuenschwander, and I'm the senior director of user privacy and child safety at Apple, where I've been a software engineer for 19 years. I worked as the first data analysis engineer on the first iPhone, and I founded Apple's privacy engineering team. Today, my job is to make sure that Apple's products and services keep our users' information safe. Thank you for the opportunity to speak with you today.

As you know, this may be one of the last times we're permitted to discuss the consequences of this legislation publicly. That's because of the bill's secrecy provisions, which forbid companies like Apple from even discussing, with our users or the public, the orders we receive.

Today, I want to be clear about how we approach privacy at Apple. I want to be clear about why encryption is so important to defending the privacy and security of people in Canada and around the world.

These issues have never been more important because our world is becoming more digital by the day. As users, we depend on our technology to securely store and process highly sensitive data like health metrics, photos and the locations of our loved ones. The places where we keep our money, store our files and conduct business are increasingly online and, sometimes, only online. The critical infrastructure we often take for granted, from the electric grid to transportation networks, is increasingly dependent on connected devices as well.

However, as technology evolves, so do the bad actors trying to steal our data. Canada has witnessed this first-hand. In 2023, Canada was one of the countries most frequently targeted by ransomware attacks. Just last year, malicious actors targeted Canadian telecom and other networks as part of the massive Salt Typhoon attack, not to just steal customer data but to also conduct broad espionage and to control the communications infrastructure that billions of people rely on every day.

As a technology company, Apple is constantly working to anticipate and prevent these threats. As an engineer, I can tell you that end-to-end encryption is one of the most effective security technologies available to defend against them. Encryption protects Canadians from identity theft, fraud, unlawful surveillance and data breaches. It protects critical infrastructure. It protects the data and communications Canadian businesses and government rely on, which are crucial to Canada's economic success and national security.

Our users trust Apple with their most sensitive information. They expect and deserve the strongest protections. That's why we're so concerned about the threat to encryption posed by Bill C-22. As drafted, this bill allows the Government of Canada to force companies to break encryption by inserting back doors into their products, something Apple will never do.

I want to be clear that we share the government's commitment to the safety and security of all Canadians. We have a team of dedicated professionals on call, 24 hours a day, to assist law enforcement. From 2020 to 2024 alone, we received just over 3,200 Canadian government requests for information, about 35% of which were emergency requests. We're committed to supporting law enforcement's work to keep Canadians safe, and we're committed to encryption technology for the same reason, to keep Canadians safe.

Again, speaking as an engineer, I do not know of a way to deploy encryption technology that provides access for only the good guys without creating new ways for the bad guys to break in. In other words, when you build a back door into an encrypted device, anyone can walk through, and because so much depends on encryption, we can't take that risk.

Look no further than Salt Typhoon. The United States passed a law requiring telecommunication companies to build access points for law enforcement into their systems, which state-sponsored actors then exploited. That law was narrower than Bill C-22, so imagine what could happen if more companies were required to create these vulnerabilities.

Apple has provided a written submission outlining targeted amendments that would improve the bill, which I'm happy to discuss. We urge the committee to adopt amendments that would, in particular, explicitly prohibit any requirement that would weaken, bypass or undermine end-to-end encryption. We believe these changes would still expand lawful access and provide Canadian law enforcement with new tools to fight crime in the 21st century.

Again, thank you for the opportunity to speak today, and I look forward to your questions.

● (1655)

The Chair: Thank you very much.

Let us turn now to Tamir Israel for five minutes, please.

Tamir Israel (Director, Privacy, Surveillance and Technology Program, Canadian Civil Liberties Association): Mr. Chair and honourable members of the committee, good afternoon. I thank you for inviting me to speak before you today on Bill C-22, an act respecting lawful access.

Part 1 of Bill C-22 represents a meaningful improvement over its predecessor legislation; however, elements of part 1 continue to suffer from overbreadth. These include the use of low standards for judicially authorized access to sensitive subscriber data and a framework that invites unconstitutional collection of publicly available data.

Elements of part 1 also allow Canada to adopt at least one, if not two, international information-sharing agreements, despite a growing tendency to use these tools for cross-border repression and an absence of comparable safeguards.

CCLA is filing a joint brief with Kate Robertson and Cynthia Khoo from the Citizen Lab, which will elaborate on these and other problematic elements of Bill C-22. I'll focus the remainder of my remarks this afternoon on part 2 of the bill, which would enact the supporting authorized access to information sct, or SAAIA.

At various points in time, governments have sought to expand their surveillance capabilities at the cost of cybersecurity, with encryption being a recurring target. Too frequently, these expansions have been justified by the expectation that surveillance capabilities will only be used by lawfully authorized government agencies and not malicious actors, yet time and again, this expectation has been proven false. The Salt Typhoon attack is the latest and perhaps the most potent reminder of this hard lesson.

It's also notable that the case for this legislation has not been made. Indeed, half of our Five Eyes partners have limited their surveillance capability regimes to imposing wiretapping obligations on telecommunications carriers. With a troubling historical track record in mind, SAAIA is fundamentally flawed in three interrelated ways.

First, SAAIA is exceedingly broad. It applies to any provider of any service that has a digital component. Under the Australian version of this law, everything from a fast-food chain that provides its customers' Wi-Fi to an electronics store that helps maintain customers' phones and computers, to any retailer that has a mobile phone application or online website, has been listed as an anticipated target.

SAAIA is also broad in terms of what obligations the government can impose. These range from requiring the ability to covertly reset customer passwords or requiring an automatic tool that generates realistic undercover profiles on social media platforms to requiring the ability to block a target's use of encrypted private messaging services in order to force them to use insecure alternatives.

SAAIA's metadata retention mechanism is equally broad. Services can be required to retain a detailed record of every single person's movements, interpersonal interactions, what applications they use and more. This is highly sensitive data.

Second, stay of limitations and safeguards fails to constrain the multiple ways that privacy, encryption and other data protections might be compromised in light of the law's broad scope. SAAIA's systemic vulnerability limitation, for example, would not apply to a set of algorithmic monitoring tools referred to as client-side scanning. Because these tools bypass encryption rather than compromising it directly, they fall outside the systematic vulnerability limitation as drafted. They nonetheless create systematic vulnerability in practice.

Third, courts remain the primary vehicle for authorizing CSIS and police surveillance activities, but SAAIA does not rely on judicial authorization, despite authorizing powers that frequently rival their Criminal Code counterparts in breadth. For example, if police want to force a company to keep a specific customer's metadata for 90 days, they need a court order, but to force the same company to keep the same metadata on every single customer for up to one year, the government need only impose an obligation through SAAIA. Judicial review is available and even required in some instances, but judicial review is highly deferential to government decision-making and no substitute for independent authorization, *de novo* review or full appeal rights. This is particularly the case when many of the obligations are imposed in secret, as is the case under SAAIA.

In sum, SAAIA poses a significant threat to privacy and cybersecurity. It's unclear how SAAIA's many overlapping flaws can be remedied through the highly attenuated legislative study it's receiving. Australia's technical capability regime was amended 173 times during a detailed committee study. Despite these changes, they were still held to be likely incompatible with human rights and a mandatory assessment of the legislation.

We therefore urge you to recommend that the government advance Bill C-22 without part 2. This legislation will be in place for years to come, and it's critically important that we get it right. The stakes are simply too high.

Thank you. Those are my opening comments, and I invite your questions.

● (1700)

[*Translation*]

The Chair: Thank you, Mr. Israel.

I now give the floor to Ms. Jeanette Patell for five minutes.

[*English*]

Jeanette Patell (Director, Government Affairs and Public Policy, Canada, Google): Good afternoon, Mr. Chair, vice-chairs and honourable members of the committee.

My name is Jeanette Patell, and I'm the director of government affairs and public policy for Google Canada. I'm joined today by Kate Charlet, a senior director on Google's public policy team, where she leads our work on cybersecurity, privacy and child safety. Before coming to Google, she spent a decade in national security roles at the Pentagon and White House.

Google is committed to supporting the efforts of law enforcement in protecting the public against crime and terrorism. We firmly believe that improving public safety and maintaining user security are highly compatible goals.

As a global leader in building safe and secure products, we take the privacy and security of our users very seriously. Our business is built on the trust our users place in us to keep their data safe. Google products are private and secure by design, protected by multiple layers of security and leading technologies, such as encryption.

I want to be unequivocally clear that Google has never built a back door or any other mechanism to circumvent end-to-end encryption in our products. When we say a product is end-to-end encrypted, it is.

In today's rapidly evolving threat environment, we believe it is critical to find ways to support law enforcement's important work without engineering vulnerabilities into products and services that weaken security for everyone.

Within this context, Google has significant concerns with several elements of part 2 of Bill C-22 as it is currently drafted.

First, the proposed regime contemplates obligations and order-making powers that are unduly broad and practically boundless. It goes well beyond lawful access regimes in other G7 democracies and risks creating new surveillance infrastructure that would introduce serious security vulnerabilities, undermine user trust and hinder our ability to innovate and offer pro-privacy technologies.

Second, the proposed framework for secret ministerial orders is unprecedented and undermines accountability and user trust. Part 2 gives the Minister of Public Safety sweeping powers to issue secret orders mandating providers to create or maintain data interception capabilities, while permanently prohibiting companies from disclosing the existence of these orders. As written, this could give the government the power to secretly force companies to redesign products to include invasive surveillance capabilities, and to do so without sufficient safeguards or oversight.

Ministerial orders are not only alarming but also unnecessary. Canada already has an effective, transparent system where law enforcement can apply to the courts for reasonable assistance orders subject to judicial oversight. Secret orders are out of step with other democratic countries and would severely restrict companies' abilities to be transparent with users about how their data is protected.

Third, the bill's definition of “systemic vulnerability” is dangerously narrow. The legislation sets a very high bar, only recognizing a “substantial risk” of unauthorized access as a vulnerability, while ignoring severe risks to data integrity and availability. The current definition fails to explicitly protect the comprehensive security measures that Canadians rely on, which go far beyond encryption.

Without stronger definitions, the law could be used to force the dismantling of critical privacy architecture, such as breaking encryption, overriding users' data deletion controls or building remote access capability, all of which could facilitate foreign interference and weaken global user privacy. At a time when cyber-threats are increasing in frequency and sophistication and malicious actors are using AI tools to find and exploit vulnerabilities more quickly, we cannot afford to be creating new vulnerabilities.

[*Translation*]

Finally, the bill imposes overly broad requirements regarding the retention of metadata, without any geographic, temporal or targeted criteria. Such requirements would mandate the blanket and indiscriminate retention of people's communications data and risk treating the entire population as potential suspects.

Unnecessary data retention threatens the fundamental rights and freedoms of Canadians, infringes on their privacy and creates a massive trove of sensitive data that amplifies the consequences of any potential security breach. The existing provisions for targeted retention orders in the Criminal Code already meet law enforcement needs while respecting the rights guaranteed by the charter.

[*English*]

To ensure that Bill C-22 achieves its public safety objectives without compromising the digital security of Canadians, Google has submitted a number of legislative amendments. We'd be pleased to discuss them today.

Thank you for the opportunity to contribute to this process. I look forward to your questions.

● (1705)

[*Translation*]

The Chair: Thank you very much, Ms. Patell.

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

[*English*]

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

Mr. Neuenschwander, first of all, thank you for being here, and thank you to all of the witnesses. It's rare to get an engineer with your qualifications here. I feel like we could have a whole hour just with you.

Have you been monitoring the committee process on this bill, may I ask?

Erik Neuenschwander: The team has. We've been keeping abreast. I was here in the prior hour.

Frank Caputo: I'll be very direct. My view is that this matter has been quite rushed. There are a lot of questions and things like that. Do you share that perspective?

Erik Neuenschwander: We're here to engage with the committee with whatever time it has.

Frank Caputo: Would it be helpful if the committee had more time to discuss this bill, in your eyes?

Erik Neuenschwander: Again, I'm just happy to be here and to answer questions, as we will.

Frank Caputo: Mr. Israel, can I ask you that same question, please?

Tamir Israel: It would certainly be helpful to have more time. This committee has had three sitting days to hear from witnesses. That's not sufficient for legislation with this level of complexity.

I mentioned the review that the Australian version of this got. It was much more comprehensive. This committee studied Bill C-8 for two months maybe, and it's a similar regime that raises similar questions but of less complexity and scope. I would say, yes; more time is needed to study this bill.

Frank Caputo: Yes, I think that this bill is actually much more technical than Bill C-8 because, with Bill C-8, we could understand what different components meant. I think we'll have a witness in the next round who actually talks about what metadata is.

We actually haven't gotten into the technical aspects of this. We have largely heard from people like you—people from Google, people from Apple—about their concerns, but we haven't even had time to delve into the technical aspects as to what this encryption means. Is that with respect to all aspects? Is it end-to-end encryption? I'm not an expert on these things, and we haven't heard about that data or about that analysis from experts. I'm quite concerned.

Mr. Neuenschwander and Ms. Patell, you can weigh in on this. The minister was equivocal when I asked about encryption. Even though we as Conservatives will be putting forward amendments that will clearly say that encryption will be offside when this bill is studied clause by clause, are you still concerned with respect to this bill touching encrypted technology?

Erik Neuenschwander: We would welcome that amendment and seeing it, but we do have concerns that go beyond encryption in terms of how risk is being looked at. As strong encryption protects all users of our services, not just Apple's but across the industry, we think it is critical that this remain protected as Bill C-22 moves forward.

Frank Caputo: Ms. Patell, do you have a comment on that?

Jeanette Patell: Yes. In a similar vein, we've put forward a number of suggested recommendations in terms of how to strengthen this bill. I think encryption is one area that we could speak to, but like Apple, we would point to the definition of “systemic vulnerability” as an area that could be strengthened, as well as the sweeping ministerial orders.

I know that my colleague, Kate, would be happy to speak more to how that could be strengthened to be more consistent with international [*Technical difficulty—Editor*].

Frank Caputo: I'm going to ask a question on that. One of the issues that I see here is that the government has tried to put in a check and balance in the form of the approval by the intelligence commissioner, though the order would remain secret. I think judicial review is actually the ultimate form of check and balance. W

hat do you say to that, either Ms. Charlet or Ms. Patell?

Jeanette Patell: I'll turn to Kate to speak to the need for oversight.

Katherine Charlet (Senior Director, Privacy, Safety and Security, Government Affairs and Public Policy, Google): Thanks very much for the question.

I do believe that it's instructive to look at some of the models that are out there. Judicial oversight certainly is an important protection. It is not the only protection. If you look at U.S. law, for example, it does require a federal judge to review before ordering a technical modification. The EU electronic evidence regulation explicitly states that any obligation to decrypt data or re-engineer systems for access is not part of the powers. The U.K. Investigatory Powers Act does include a judicial commissioner review.

None of those protections is available in Bill C-22. We recommend that a judicial review be a part of this, but it is perhaps not the only safeguard that could be added here.

● (1710)

Frank Caputo: Along those lines, would you agree....?

This is an exercise in comparative legislation and drafting. One of the deficiencies I think we've had in this committee process is that we haven't heard from experts on EU law or on Australian law, where they keep metadata for even longer but I don't know exactly what categories of metadata they're keeping. Do you see it as a deficiency in this study when we don't actually have people from other jurisdictions, which is something that we heard about from the committee process?

Would it concern you, as an outside observer, that this committee isn't looking at other models and hasn't heard from witnesses who are experts on other models so that we can compare them in order to get the best possible outcome?

Katherine Charlet: I do agree that it's instructive to look at those other models.

From our assessment, it does appear that Bill C-22 would be the only G7 regime that does not include judicial oversight but does have the expansive ministerial order powers. Certainly others could weigh in on this as well, but I do think it's an instructive part of the conversation.

Frank Caputo: Thank you.

The Chair: Thank you very much for that.

Let me turn to MP Zuberi for six minutes, please.

[*Translation*]

Sameer Zuberi (Pierrefonds—Dollard, Lib.): Thank you, Mr. Chair.

[*English*]

Mr. Israel, I would like to pick up on the last comment by Ms. Charlet. Given that you're in the Canadian Civil Liberties Association, can you comment on what Ms. Charlet just said with respect to what other jurisdictions are doing?

Tamir Israel: The Australian regime does not include judicial authorization. This has been one of the heaviest criticisms levelled at the regime, including by an independent review of the regime that was conducted two years ago. It was the single biggest flaw that the independent review considered needed to be fixed right away. The U.K. regime does rely on judicial review by a commissioner.

Under Canadian law, judicial review, as a mechanism, is different from judicial authorization, and it's important to keep the differences in mind. Judicial review is an assessment of whether the decision-maker made a reasonable decision based on the information in front of them. In contrast, when judges are authorizing a search warrant or something of that nature, they are the ones who are weighing the different considerations.

Given the nature of the bill, it's particularly problematic to rely on judicial review alone, as opposed to a stronger type of independent scrutiny.

Sameer Zuberi: In other Five Eyes or comparable jurisdictions, is there judicial authorization in advance or only judicial review?

Tamir Israel: In the U.K., it's judicial review, although the mechanisms of judicial review may differ from what's here in Canada. That regime is currently under constitutional challenge.

In the U.S., the entire regime is overseen by an independent regulator—the Federal Communications Commission—so that's more comparable to judicial authorization.

Sameer Zuberi: Thank you.

Mr. Neuenschwander—

Erik Neuenschwander: “Erik” is also fine.

Sameer Zuberi: Erik, in terms of what we just heard, are you familiar with other jurisdictions and how they're dealing with these concerns to balance catching bad actors online and protecting civil liberties? Are you familiar with what other jurisdictions are doing?

Erik Neuenschwander: From an engineering standpoint, I am in terms of the scope of what the orders might be able to request.

Sameer Zuberi: With respect to the legislation and the engineering standpoint that you mentioned you're familiar with and that exists in other jurisdictions, do other jurisdictions have the concern that we have, in the sense that we cannot necessarily catch all of the bad culprits that we should be catching within a reasonable period of time, and this legislation seeks to shorten and address that concern about a reasonable time?

● (1715)

Erik Neuenschwander: It's hard for me to speak for other jurisdictions, but in general, I would say that the desire to catch bad actors is a universal one.

Sameer Zuberi: I ask because the comparative is interesting.

Ms. Charlet, if you have knowledge on this particular question, then feel free to answer. Otherwise, I'll continue to other questions.

Katherine Charlet: Google appreciates the challenges that law enforcement faces, and we're here to support those efforts. That's part of our effort to provide constructive recommendations on how to amend the bill.

Sameer Zuberi: Erik, earlier you mentioned encryption. We've heard many times from the government's perspective that it is not being asked that encryption be unlocked.

How is it that you still are coming to the committee and the main thrust of your testimony is around encryption and your concerns about it being unlocked? How do you square that circle?

Erik Neuenschwander: Again, I'm certainly not an expert on legislative text, but in reviewing it with the team, I don't see anything written within the bill itself that provides those protections against encryption. I do grant that the bill does not actually specify what these orders would do. That's kind of left for later.

To bring this into a real-world analogy, I might say something like we're concerned about a hole being put in a wall. I would say that the bill does not put a hole in the wall. It merely allows for secret orders to force putting a hole in the wall. Our concern is motivated because, at the end of the day, there would still be a hole in the wall.

Sameer Zuberi: If your concerns, as the the government puts forth, are moot, then do you have any other amendments or suggestions with respect to the legislation that you would like to put on the table?

Erik Neuenschwander: The primary ones are around protecting encryption explicitly and strengthening the definition of systemic risk, as encryption is just one aspect of where making everyone less safe, we think, would be a counterproductive outcome for society.

We would welcome additional judicial review. We would welcome relaxation of some of the secrecy protections, because I would like conversations such as this one to still be able to occur in the future. We also have some concerns around the breadth of the inspection powers that are in the bill and the possibility of installing third party equipment into secure networks.

Sameer Zuberi: Mr. Israel, I'd like to open up the floor to you for the next few moments to add anything that you'd like to add.

Tamir Israel: A definition that encompasses the need to exclude any obligations that cause systemic vulnerabilities would need to take into account the multiplicity of ways and proposals that keep emerging for getting around encryption. Many of these don't compromise encryption directly, but try to get at it indirectly by circumventing it or bypassing it, yet still have the same impact in terms of the vulnerabilities that they ultimately create. The current definition doesn't capture all of these. It's limited in scope. I would also really encourage your committee to consider blocking that.

Sameer Zuberi: Thank you.

[*Translation*]

The Chair: Thank you, Mr. Zuberi.

Mrs. DeBellefeuille, you have the floor for six minutes.

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

I thank the witnesses for joining us.

Ms. Patell, I thank you and congratulate you for taking the time to deliver part of your remarks in French. Your French is excellent, as is your pronunciation. So, thank you very much.

Your company operates in all Five Eyes countries, if I am not mistaken. Therefore, you are already subject to legal access regimes or laws, such as those in the United States. When compared to the United States, we see that Canada has more laws, mechanisms and institutions that protect privacy. At least, that is my interpretation.

So, given that your company also operates in the United States and that you say you find the Canadian government's bill too restrictive, can you tell us how, in your view, it compares to that of the United States?

Jeanette Patell: Thank you for your question and for your kindness regarding my French.

I will now turn the floor over to my colleague Ms. Charlet, because it is clear that there is tension regarding the Privacy Act and Bill C-22.

● (1720)

[*English*]

I'll pass it on to my colleague Kate to speak more with regard to the privacy considerations that are invoked by this law in particular, in comparison with the U.S. regime.

Katherine Charlet: Thank you very much.

I think the primary comparison here is to privacy principles. We think of privacy principles around data minimization and user controls and about the potential that Bill C-22 could undermine those privacy principles.

Just as an example, if we look at Google's provision of user controls, we offer users the ability to choose to delete their data after three months. Retention requirements or product changes that require us to make changes that would require retention for longer than three months would be against the wishes of a user. We look at this with concern in terms of privacy principles that are global in nature.

On your question regarding U.S. law, we look to U.S. law—CALEA specifically. CALEA does explicitly forbid governments from forcing a company to break encryption. That is a similar protection that we would be seeking in Bill C-22.

[*Translation*]

Claude DeBellefeuille: Experts and civil society organizations say that the U.S. CLOUD Act grants U.S. authorities the power to demand access to data held by companies subject to U.S. law, regardless of where the data is stored.

If Bill C-22 is passed, do you believe Canada will be equipped to deal with this requirement? Many companies and citizens are afraid. They fear that, once Bill C-22 is passed, our data will become accessible to countries that do not share our concerns regarding privacy protection or even respect for human rights.

[*English*]

Katherine Charlet: I would say that this law does have global impact. Bill C-22 could require, under the ministerial orders, a company to make product changes. It is essentially unbounded in terms of what those product changes could be, as well as the secrecy requirements involved. Google and other companies are global companies and Canadians interact with people all over the world, so there are global impacts to a proposal such as this one.

[*Translation*]

Claude DeBellefeuille: Ms. Charlet, you say that Bill C-22 is more intrusive in terms of legal access than the laws in the United States.

[*English*]

Katherine Charlet: Yes, ma'am.

The essentially unbounded nature of the powers that are afforded to direct product changes by companies in secrecy and without judicial oversight, in the case of the ministerial orders, goes beyond any regime that I'm familiar with.

[*Translation*]

Claude DeBellefeuille: Were you consulted prior to the drafting of Bill C-22?

Did you express your concerns to the government during the bill's drafting process?

[*English*]

Katherine Charlet: We have provided a submission with some specific recommendations, but I will pass this to my colleague, Jeanette, on your broader question.

Jeanette Patell: We have shared these concerns with the government. I don't believe we were in a consultation process prior to tabling, but we welcome the opportunity to engage with this committee to find workable solutions here that can support law enforcement in its legitimate need to conduct investigations, while also preserving user privacy and maintaining the security of our products and services.

Thank you for the constructive engagement.

The Chair: Thank you, Madame DeBellefeuille.

We'll now go to Ms. Kirkland for six minutes, please.

● (1725)

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

I would like to start with just—

The Chair: I said six, but it's five minutes.

Rhonda Kirkland: You said six, so it's too late. I want those seconds back, though.

I'd like to start by talking about the fact that this is rushed. We've mentioned this before. It feels rushed to me as a parliamentarian. I had questions in the last hour that I really wanted to get to and wasn't able to because of how fast all this is proceeding. I made the statement early on that I thought we should be careful not to just race to royal assent. If we're going to do this, then we need to get it right.

I know that we've missed getting some submissions to the committee, and I don't fault anyone for that. I know there was no malice intended. I don't fault the clerk for that. It's to be expected in such a rushed environment that those types of things will happen.

Mr. Neuenschwander, it is my understanding that you did provide submissions to this committee. I don't believe it has come through the clerk yet, but thankfully, you sent them to each of us directly. I appreciate that very much.

I want to backtrack with regard to what I hear over and over again, the term "back door". I think Canadians really need to understand what that means.

On the Government of Canada website from five days ago, under lawful access, it says, "Bill C-22 does not require ESPs to create 'backdoors' to their systems or [to] weaken electronic protections, including encryption."

Also said in testimony by Mike McGuire was:

> This part does not create new powers for law enforcement or CSIS to intercept communications or obtain information, nor does it allow direct government access to electronic service providers' systems. It also explicitly prohibits the creation of systemic vulnerabilities, to ensure that a regulation or ministerial order does not weaken encryption or create back doors.

The minister said:

> This part also includes an explicit safeguard to prevent the introduction of systemic vulnerabilities in electronic protections. Our government does not support the creation of back doors.

Testimony today seems to make that obviously not really the case, so I need some clarification. I'm happy for each one of you to provide that clarification. I think the word "explicit" is worth taking a longer look at, because it doesn't seem to be explicit in this legislation. I know that there are ways that we can make it explicit, so I'd like each of you to talk about that briefly. Thank you.

We'll start with Mr. Neuenschwander.

Erik Neuenschwander: I did not hear that testimony directly, but in our reading of the bill, we don't see some of those claims explicitly in the language. There's not a mention of protection of encryption, which we would support being added to the bill. In the definition of systemic risk or "systemic vulnerability", it mentions the term but without a definition of that term.

The intentions aren't coming through clearly in the language, from our perspective. That's why, as you've mentioned, we've given a written submission and suggested amendments.

Rhonda Kirkland: Thank you.

You used a very important word, which is "intention". We're often told that this bill does not intend to do X, Y or Z. I'll say again that Canadians really don't care what the bill intends to do. They care about what the bill will allow the government to access, and that's a real concern. Thank you for bringing that up.

I'll take it to Mr. Israel first, and then we'll go on to Google.

Tamir Israel: I echo your concerns about intent versus application. It took seven or eight years before the U.K. version of this law was used to strip all people in the U.K. of a critical encryption safeguard for their Apple iCloud backup. It's not the immediate intent of the government that's relevant. It's how the bill could be applied over time.

In this instance, the bill does prohibit the imposition of systemic vulnerabilities, but that, by definition, does allow non-systemic vulnerabilities, first. Second, it leaves a lot of e-terms in the definition open to interpretation through regulation.

A big problem with the constant attempt to maintain end-to-end encryption secure is the multiple ways that governments and bad actors keep coming up with to get around encryption. Some of these mechanisms directly compromise encryption. I've seen government definitions of back doors limited to those examples, but other tools that are commonly advanced, for example, client-side scanning, which essentially places an AI tool on everybody's device that monitors their content before it's encrypted and sent onwards and has been assessed by leading security technologists around the world as creating systemic vulnerabilities, do not compromise encryption in the way that this exception would prevent. You need a comprehensive exception that rules out all back doors and all ways of bypassing encryption.

Thank you. I'm sorry for the long answer.

● (1730)

The Chair: Thank you, Ms. Kirkland.

We'll go to MP Housefather for five minutes, please.

Anthony Housefather (Mount Royal, Lib.): Thank you very much.

Mr. Neuenschwander from Apple and Ms. Patell from Google, I appreciate your testimony and your being here. I've read your submissions. As a general counsel for a computer company before I went into politics, I'm sympathetic to strengthening protection for encryption and clarifying the definition of "systemic vulnerability" and some of the other provisions you mentioned.

I want to respond to something Ms. Kirkland said. Authorities provisions are standard in any compliance framework. They are in many federal laws, and they don't really specifically relate to the core lawful access provisions of this bill. I just wanted to get that out.

Mr. Neuenschwander, I've read what you said. Has Apple ever gone before a parliamentary committee or made a submission to a national parliament on a lawful access regime that Apple actually supported?

Erik Neuenschwander: I'm more on the engineering side than our government affairs side. I'm not familiar with all of our submissions, but we are supportive of parts of Bill C-22 and modernization overall to enable law enforcement to become better and more efficient—

Anthony Housefather: I understand that. I understand that both Apple and Google are largely supportive of the idea but have objections to specific provisions of the bill. I just wanted to establish whether you have ever seen a bill that you didn't have objections to some portions of.

I think people are overstating some of the objections. I don't disagree with some of the objections you raised, but I don't think some of the claims that are being made—for example, surveillance equipment that could be installed in devices and forcing companies, even under orders, to put in surveillance equipment—are reasonable or logical. I don't think they bear out in the wording of the bill.

What I'm asking is this: Have you guys ever gone before a committee or made a submission in the U.K., in Australia or in the U.S. and said, "Wow, we think this bill is great"?

Erik Neuenschwander: As we're doing here today, we have frequently gone to engage in constructive—

Anthony Housefather: Yes, you've gone to engage and to object to provisions in the bill, which is your job.

We as legislators have to look at it with multiple lenses. You have a specific obligation related to the company. The company's obligation is often to respect its user agreements with end-users and to do what's best in the company's interest, not necessarily in the national interest.

All I'm asking is if you have ever come to a committee and said, "The bill is great." I doubt that you have.

Erik Neuenschwander: With respect, I think we're trying here to act in the interests of users, both Canadian and worldwide, and ensure that we can provide the strongest protections possible while supporting law enforcement.

Anthony Housefather: I don't disagree with you. I think that's part of the overall goal.

Let me also ask.... You are the chief privacy officer. You're in charge of privacy at Apple.

Erik Neuenschwander: I am from the engineering standpoint, yes.

Anthony Housefather: It's from the engineering standpoint. That's right.

You may think this is a negative question, but I don't. I think this is actually a lesson.

Has Apple ever created something that you later regretted? With respect to privacy interests, I'll give you the IDFA as an example.

Erik Neuenschwander: I don't know that I would go so far.

For those less into the technology, the IDFA is an advertising identifier. I think it was appropriate for its time. What we do is we continue to evolve the protections on the privacy and security side as the world continues to change.

Anthony Housefather: You did create something that eventually had ramifications that you and your team probably didn't even realize when you first created it. Developers actually used this to thwart what you thought would be users' preferences. I remember that.

Erik Neuenschwander: I take it as a given that attacks and uses of data only increase and grow stronger over time, which is why we continue to move forward and innovate on the protection side. I wouldn't put IDFA in the class of attacks, but when we're thinking about attacks generally, we have to continually move forward to continually protect against the stronger attacks.

Anthony Housefather: I agree, and that's why, when we look at this bill, we have to look at some of the concerns that are being raised, even if we don't necessarily think that those are likely to happen. We know that we have to provide for contingencies. We have to make sure that we avoid getting ourselves into a situation where pernicious effects could occur. I'm actually sympathizing with what you're saying, because whether it's in the bill or not, I think we want to provide for the concerns that are there.

Ms. Patell, I carefully read your submission as well. If we were able to limit the definition of “systemic vulnerability” and we were able to guarantee or make it clear that encryption was not to be broken, would those be the two major points that you would have with respect to the bill that would alleviate the concerns that Google has expressed?

● (1735)

Jeanette Patell: We certainly welcome all of the statements that have been made with regard to the government's intent, and specifically with regard to the desire to protect encryption. We simply want to see that reflected in the text of the bill itself.

I would point to a few other areas where we've put forward four recommended amendments. A few others relate to both the metadata retention provisions and to the sweeping nature of the ministerial orders. That's something that we believe is unprecedented and unnecessary, and we would therefore recommend the elimination of secret ministerial orders as well.

I don't know if my colleague Kate wants to weigh in as well on anything else.

Anthony Housefather: I think the chair might not allow that since it seems as though my time is up.

The Chair: I'm sorry. Unfortunately, your time is up, Mr. Housefather, so is the time for answering those great questions.

[*Translation*]

Mrs. DeBellefeuille, you have the floor for two and a half minutes.

Claude DeBellefeuille: Thank you, Mr. Chair.

Mr. Israel, do you share these concerns? In your view, does the bill increase the risks associated with sharing information with states that have a troubling human rights record?

[*English*]

Tamir Israel: Yes, in two respects. First of all, the bill paves the way for the adoption of international information-sharing agreements, including with countries that have problematic human rights records. That's one problem.

A related problem is that the metadata retention regime has no limitations on who can access that metadata. Once it's kept, any government can force a multinational company that's active in their jurisdiction to disclose that data, which would not have been kept if the company was not forced to keep it, about people in Canada.

[*Translation*]

Claude DeBellefeuille: In that regard, have you ever expressed your concerns to members of the government regarding the exchange of personal information with states that have a rather troubling human rights record? This is not the first time you have expressed such concerns to members of the government.

[*English*]

Tamir Israel: We've expressed our concerns regarding the information agreements I mentioned. However, we were not made aware of the inclusion of the mandatory data retention regime until Bill C-22 was tabled, so we did not have a chance to mention it in advance.

[*Translation*]

Claude DeBellefeuille: In your opinion, should we give more powers to accountability and oversight bodies to monitor government activities and better protect users’ privacy?

[*English*]

Tamir Israel: Absolutely. I think judicial authorization will be a critical addition here. Having more direct oversight from bodies like NSIRA and the Office of the Privacy Commissioner would also be helpful. This is a very powerful set of tools that are being brought into place.

Also, as a civil liberties organization, we don't appear at many legislative committees to encourage an expansion of police powers. However, I do want to say that we are very selective in when we show up and how aggressively we object. This regime really is on the broader end, which is why we are here and expressing our concerns.

[*Translation*]

The Chair: Thank you, Mrs. DeBellefeuille.

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

[*English*]

Roman Baber (York Centre, CPC): Thank you.

Erik from Apple Inc., welcome to public safety and national security.

I see a comment, which was made by the Apple company, in The Globe and Mail that this legislation could allow the Canadian government "to force companies to break encryption by inserting back doors into their products—something Apple will never do."

For the record, Conservatives oppose the breaking of encryption. However, I'd like you to follow up on this comment by Apple that breaking encryption by inserting back doors into your products is something you would never do. Let's say that this legislation passes in its current form and the Liberals get their way. What happens then?

● (1740)

Erik Neuenschwander: We will remain committed to providing the highest level of security we can for Canadians. We hope that the bill will be amended to provide those explicit protections for encryption so as to avoid putting those things in tension.

Roman Baber: I appreciate that, but what if Conservatives are unsuccessful, and you're forced to insert a back door and break encryption? What will Apple then do? Will that be a first for Apple, or will that mean that Apple will be leaving Canada?

Erik Neuenschwander: I can't speculate what would happen in that situation. Through this engagement and the continued dialogue we hope to, again, have positive amendments made to the bill.

Roman Baber: Can you tell us what happened in the U.K. vis-a-vis the same question, when Apple decided that the legislation in the present form was unacceptable to it?

Erik Neuenschwander: Apple filed comments in both the initial round of the bill and then as public comments during its amendment phase, more recently.

Roman Baber: Okay.

To Google, I see in your brief a comment that, "Google has never built a back door or any other mechanism to circumvent end-to-end encryption in our products." Is that limited to Canada, or is that global?

Jeanette Patell: That is global.

Roman Baber: In other words, this would be a first. If this legislation is successful and if it passes in its current form, Google would be forced to do something it has never done anywhere in the world.

Jeanette Patell: If this legislation passes in its current form, the minister would have the power to order Google or any other electronic service provider to comply with the core obligations that are listed in proposed subsection 5(2).

We're here today to ensure that the committee takes the time to have this conversation and arrive at a piece of legislation that is workable and strikes the right balance in preserving user safety and security while supporting law enforcement efforts.

Roman Baber: Thank you.

You write that the scope of these potential obligations is largely "boundless". Could you tell us some of the boundaries that may be tested here that have not been tested before, other than the breaking of encryption?

Jeanette Patell: There are in fact comprehensive layers of security architecture that are at stake here that go well beyond encryption.

I think my colleague Kate can speak to what that could entail.

Katherine Charlet: I'd say the reason that we view these as essentially boundless is that the powers for the ministerial orders as well as the core provider obligations really are essentially boundless in the sense of the notices that could be given to persons; the installation, use, operation, management and testing of any device or equipment; and numerous other enumerated powers that go beyond some of the authorities that are given in other countries around the world.

Roman Baber: If I understand your submission correctly, not only is the scope of those ministerial orders potentially boundless, but the framework for these ministerial orders also immunizes them from any appropriate scrutiny or accountability, because you can't appeal them.

You can't go to a court and say that you're not comfortable doing what the minister orders you to do. There is no judicial oversight. Is that correct?

Katherine Charlet: It's correct that this is done entirely in secret.

I do believe that there is an ability to appeal. However, during that appeal period, there is no stay, so if there is an order on the company, the company would be obligated to implement the change before getting a decision on an appeal.

Roman Baber: I want to clarify that the public safety minister, the government, CSIS and the RCMP already have an ability to seek and obtain a search warrant and ask Google to comply with requests for information. Is that correct?

Katherine Charlet: That is correct.

Roman Baber: Then I'm not exactly sure why there is the requirement to overbear.

I want to talk for a minute about the electronic—

The Chair: Unfortunately, the time is up, MP Baber. I'm sorry for that.

Let me turn to MP Powlowski for five minutes, please.

Marcus Powlowski (Thunder Bay—Rainy River, Lib.): Because I'm a boomer, my kids can run circles around me with respect to everything involving computers, and I have to say that I'm still trying to figure out this bill.

The bill pertains to service providers and data providers. Is Apple one or both of those, Erik?

● (1745)

Erik Neuenschwander: I might guess so, but it seems unspecified within the bill.

Marcus Powlowski: How would you define a service provider and a data provider?

Erik Neuenschwander: I don't count myself as an expert on legislative text, but I would think that it's trying to look at service providers that hold information as part of doing business.

Marcus Powlowski: I'm sorry. Is that the service provider and the data provider? Maybe I don't need to ask you that.

Tell me about the cost implications of this bill for Apple. How is this going to affect you financially?

Specifically, there is a requirement for retaining metadata for up to a year. You're a computer guy. You're an engineer. How do you maintain metadata? Where does that happen? Is that up in your cloud? Where does that take place, and what are the costs for your company in keeping that kind of data?

Erik Neuenschwander: Primarily, I don't think we're overly focused on the costs. We're focused on the risks that would arise from that increased metadata retention.

Currently, we maintain the minimum amount of data necessary to provide the service. My understanding from the current draft is that it could force an increase beyond that time. What we're looking at then is just a larger amount of data that could be breached by an attacker and used to commit other crimes.

We're not aware of that ever having happened to Apple so far, and I will touch wood, but part of that is because we reduce that threat profile today as much as possible.

Marcus Powlowski: You do not think the cost implications are of concern to your company.

Erik Neuenschwander: As an engineer, it's probably a little outside of my area, but again, I would be concerned mostly with security.

Marcus Powlowski: Let me ask Google the same question.

Do you consider yourself a service provider, a data provider or both of those?

Jeanette Patell: Similar to Apple, some of those definitions are left for future regulation, so we await further clarity in terms of the scope. Our understanding is that, either way, we would be captured by the legislation.

Marcus Powlowski: I'm a little surprised. Given the size of Google and Apple, how big these companies are, I'm a little confused that legislation can be so vague that you don't even know whether this applies to you.

Jeanette Patell: It's a very good point about the opportunity for clarity and precision in the legal text so that the companies that are operating in Canada have a clear sense of the obligations that apply to them.

Marcus Powlowski: Can I ask you about the cost implications of this? Maybe I should ask generally before I get into the specifics of retaining metadata for up to a year. Just generally, what do you see as the cost implications for Google?

Jeanette Patell: Similar to Apple, the cost considerations have not been our primary consideration. We've been focused on the vulnerabilities that this would introduce to our—

Marcus Powlowski: Let me challenge that. You are corporations. I think you do very well as a corporation. I may even have stocks in your corporation, which—thank you very much—do very well, but I think you are driven and mandated as a company to look after the financial bottom line. I'm a little surprised that you're not concerned about the financial implications of this.

Jeanette Patell: Our goal here is to first preserve users and the systems that we operate. We invest quite a lot of resources in doing that for users globally, including from some of our incredible team out of Montreal.

Maybe Kate can speak to what we see in terms of the compliance burdens that might come with regimes like this.

Katherine Charlet: I agree with the comments made so far on cost, but what I would add is that global companies seek to build one product experience, not have 100 different product experiences and systems that they have to build around the world.

Of course, we're a large company. We can handle complex compliance regimes but, in terms of the product experience, it's a better experience for users when they move across borders to have a similar experience.

Marcus Powlowski: We've already heard that—

The Chair: I'm sorry, MP Powlowski, to cut you off, but that's my obligation, given that the time is over for this second hour.

Thank you, witnesses, for taking the time to be with us either in person or virtually.

We will suspend for a few moments until the other group comes in. Again, thank you, and have a great day.

● (1750)

_____(Pause)_____

● (1755)

[*Translation*]

The Chair: We are resuming the meeting. This is the third part. We are welcoming new witnesses, to whom we extend a warm welcome.

We welcome Mr. Mathias Van Laer from the Royal Canadian Mounted Police, who is here with us.

[*English*]

I invite everyone to be a bit more attentive.

[*Translation*]

From the Canadian Association of Chiefs of Police, we welcome Commissioner Thomas Carrique.

From the city of Brampton, we welcome Mr. Patrick Brown, mayor of Brampton.

I would like to welcome our witnesses.

We will now begin the five-minute presentations.

Mr. Van Laer, you have the floor.

[*English*]

Mathias Van Laer (Retired Staff Sergeant, Reservist, Royal Canadian Mounted Police): Good afternoon, Mr. Chair and honourable members of the committee. Thank you for the invitation to appear today, as we gather on the traditional and unceded territory of the Anishinabe nation and recognize the continuing presence of first nations, Inuit and Métis people in this region.

My name is Mathias Van Laer. I served as a regular member of the RCMP for 25 years and, eventually, retired in 2022 as a staff sergeant.

[*Translation*]

I would also like to point out that I am of French-speaking origin. I will be happy to answer your questions in the official language of your choice.

[*English*]

During my service, I was a non-commissioned officer in charge of the RCMP E Division's integrated child exploitation unit, located in the Lower Mainland district but representing the whole province of British Columbia. Following my retirement in 2022, I returned to the RCMP as a reserve constable for the city of Kamloops, B.C., to continue my work within their sex crimes unit, where I actively work on ongoing investigations, prepare judicial authorizations and oversee the intake of all online child sexual abuse investigations within the city of Kamloops, providing guidance, direction and training.

To provide you with some background, the RCMP's child exploitation units are specialized teams dedicated to preventing, detecting and investigating crimes involving the sexual exploitation of children, both online and off-line. Their mandate focuses on protecting vulnerable victims, identifying and apprehending offenders, and working collaboratively with domestic and international partners to disrupt networks involving child abuse material and exploitation. Key priorities include proactive intelligence gathering, victim identification and support, digital forensic analysis and public awareness initiatives to reduce risk and increase reporting.

During my time with the B.C. ICE unit, I have worked to address the growing demand, driven by the increasing use of the Internet, for online child sexual exploitation investigations. In collaboration with the RCMP's digital forensic services, B.C. ICE supports law enforcement agencies across British Columbia, works to identify and assist child victims, and identifies offenders to support appropriate criminal charges.

As investigators, we are constantly adapting investigative techniques to try to keep up with criminals, especially those who operate in the digital space and who do the greatest harm to vulnerable Canadians, including children. Bill C-22, an act respecting lawful access, would modernize our law so that Canadian police services can investigate crimes and target those who prey on the vulnerable.

RCMP child exploitation units increasingly rely on digital tools, data analysis and collaboration with intelligence partners to make progress in investigations. The Criminal Code amendments, proposed through Bill C-22, could improve timeliness and consistency in obtaining digital evidence, particularly in urgent or rapidly evolving cases.

Child exploitation investigations predominantly depend on IP address tracing, subscriber information and preserving volatile online data before it is deleted or purged. Enhanced lawful access provisions could streamline production orders and preservation demands, allowing investigators to act more quickly to identify suspects and to safeguard victims.

Protecting children remains a core priority for the RCMP. Teams are committed to safeguarding vulnerable victims, pursuing offenders and adapting to evolving online threats through strong partnerships and modern investigative tools. Whether through enforcement, victim supports or prevention efforts, the RCMP continues to place the safety and well-being of children at the forefront of its mandate, recognizing the critical importance of protecting them from harm in all environments.

Thank you very much. I look forward to your questions.

● (1800)

[*Translation*]

The Chair: Thank you very much, Mr. Van Laer.

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

[*English*]

Commissioner Thomas Carrique (President, Canadian Association of Chiefs of Police): Distinguished committee members, thank you for the opportunity to comment on Bill C-22.

Today, virtually every serious criminal investigation has a digital component. Organized crime groups, child predators, fraudsters, violent offenders and extremists rely on encrypted communications, digital platforms, anonymized tools and forum-based services to coordinate criminal activity, evade detection, frustrate prosecution and ultimately victimize innocent Canadians. Criminals are leveraging digital infrastructure and encryption, while the police are hindered by outdated legislation that does not prioritize public safety.

Bill C-22 is not about expanding unchecked police powers. It's about ensuring that judicially authorized investigations can function effectively in a complex and ever-changing digital environment. To the benefit of bad actors, too often debates on lawful access focus exclusively on privacy interests of suspects and the financial interests of big tech, while overlooking the rights of victims to safety, justice and timely intervention.

The police are not asking for, nor does Bill C-22 authorize, broad surveillance. It does not permit warrantless interception of communication. It does not eliminate judicial oversight. It does not provide unrestricted access to browser history or to social media content. The legislation preserves charter protections and maintains judicial authorization requirements for advanced investigative techniques.

Bill C-22 also addresses practical investigative steps. For example, it creates confidential confirmation of the service process with a simple yes or no so that investigators can determine which telecommunication provider actually holds relevant records before spending valuable time seeking judicial authorizations for records that simply may not exist. It creates a production order process for basic subscriber information based on reasonable suspicion, allowing investigators to advance early-stage investigations. It also addresses delays involving foreign-held evidence for cases in which investigators currently rely on mutual legal assistance processes that take many months, often while evidence disappears. In fact, Bill C-22 provides clear statutory rules in areas where courts, providers and investigators currently face inconsistent interpretations and legal uncertainty.

Bill C-22 prevents the harbouring of criminals by setting out the requirement for electronic service providers to develop and maintain systems capable of providing police with communication and information that they are legally authorized to obtain and that they require to advance criminal investigations.

It's important to note that Bill C-22 is not a surveillance tool; it's a lawful access framework. Metadata would be retained for a maximum of one year, including information such as date, time, duration and origin of transmission. It's critical to note that there will be no obligation to retain content such as emails, web browsing history or social media activities.

Furthermore, retention does not equal access. Judicial authorization will still be required. Metadata is the bare minimum of information that could assist investigators in complex investigations, such as those for homicides, international child sexual exploitation, extortion, cross-border auto theft, human trafficking and the smuggling of drugs and firearms. These types of crimes can far exceed a one-year investigation period that can involve the need for lawful access.

Absent reasonable suspicion of criminal activity, police will not and cannot judicially seek and lawfully obtain communication metadata about a private citizen of Canada going about their daily activities. Additionally, there are other safeguards built into the bill. Regulations made by the Governor in Council must consider privacy and cybersecurity implications, feasibility, cost to providers and impacts to customers, and the intelligence commissioner must approve orders prior to their issuance on an electronic service provider.

Bill C-22 also prevents any requirement that would cause an electronic service provider to introduce a systemic vulnerability, defined in the bill as "a substantial risk that secure information could be accessed by a person who does not have any right or authority to do so."

● (1805)

Frankly, from a law enforcement perspective, the concerns by some major telecommunication companies and special interest privacy advocates about encryption and cybersecurity are overstated. The legislation as written does not compel companies to weaken encryption or create vulnerabilities; rather, under a legislative framework, it ensures that electronic service providers are not serving as a safe haven for criminal and terrorist-related activity and compromising public safety locally, nationally and internationally.

The Chair: I'm sorry to interrupt, Commissioner, but could you finish in five or 10 seconds?

Commr Thomas Carrique: Absolutely, sir.

In closing, I look forward to answering your questions.

Thank you.

The Chair: Thank you. That was much appreciated.

Let us now turn to Mayor Brown.

Mayor Brown has particular merit in being here today, given that this is his birthday. We won't take the time to sing you a happy birthday, because we don't want to interfere with your allocated time.

Happy birthday, Mayor, and it's five minutes for you as well.

Patrick Brown (Mayor, City of Brampton): I was going to celebrate my birthday, but when I heard you were talking about such an important topic, I did not want to miss this opportunity to speak on behalf of the residents of Brampton and the Peel region, where we have unfortunately faced significant criminal activity and where Bill C-22 could have made a world of difference.

I want to share a few things with the committee today.

Organized crime is sophisticated. I wear two hats, one as mayor of Brampton and one as a member of the Peel Police Service Board. Commissioner Carrique's comments, which were so eloquent, were what I hear from our senior police. This could be the most significant investigative tool for police since DNA evidence changed the game.

Organized crime does not want Canada to update our lawful access legislation. Frankly, they've been able to conduct criminal activity with impunity in our country. Police have their hands tied, and it's unfortunate. There are more victims and there are more preventable crimes. I'm sure that if this committee or the Parliament of Canada dithers or delays, the Bishnoi gang will be elated, the Sinaloa cartel will be elated and For Brothers will be elated, but there will be more victims.

I come from a community where I've seen too many cases of child exploitation, human trafficking and extortions. Don't even get me started on extortions, because they have terrorized our community. I can tell you that in Peel region over the last year, we've had 476 extortions on families and businesses. This legislation is absolutely critical for us to be able to hold these criminal organizations accountable.

In the case of extortions, production orders can take three, four or five weeks, and sometimes even longer. There are continuous delays. With these delays on production orders, investigations go cold.

Police investigations are most efficient when they have the tools to do their job, and I can tell you that organized crime is utilizing all of these modern technology tools. When investigators have to wait 45 days for critical information, video from local cameras disappears, critical evidence disappears and more innocent victims are traumatized.

I've had victims call me. I had a father call me who said, “My kids can't sleep after our house was shot up.” Can you imagine having your children not being able to sleep for months because they were terrorized by an extortion? These extortions could have been prevented if the police had the tools to do their job.

I know there were concerns from the opposition over the initial incarnation of this bill. However, I can tell you—and I know the Peel police have been involved in providing input—that this is a balanced approach that gives the police the same tools as other Five Eyes countries. I know there are going to be tech lobbyists aggressively lobbying against this bill for their own reasons, but if this works in other Five Eyes countries where there is a balance between protecting privacy and giving police the tools to do their jobs, we can find that balance in Canada.

I was at the big city mayors' caucus, where we lobbied Prime Minister Carney specifically to give local police forces this tool that is so critical. For those who have privacy concerns, my message would be this: Don't commit a crime. Don't be involved in a heinous crime. Then you won't have your privacy abridged.

You hear law enforcement saying that it will be utilized only when there is reasonable suspicion of a crime. If we have video evidence of someone being involved in a crime, it shouldn't take 45 days to get that digital information.

This is the new warfare. I read these police reports and I study them. I can tell you that I have asked our senior leadership in the Peel Regional Police again and again how long this investigation would have taken if we had lawful access. Time and time again, they respond that it would be a fraction of the time. For investigations that have gone cold, this could have made a difference by actually preventing crime and preventing more victims, so I implore this committee to not dither and delay.

If there are reasonable adjustments and amendments, we have reasonable parliamentarians here. Please find that consensus, but do not dither and delay. The only people you will please with any dither and delay on this critical information that law enforcement is begging for are organized crime members.

I'm happy to be before this honourable committee today.

● (1810)

The Chair: Thank you, Mayor Brown.

Let us now turn to MP Caputo for six minutes, please.

Frank Caputo: Thank you.

Happy birthday, Mayor. It's nice to make your acquaintance over Zoom.

It's nice to see you again, Commissioner Carrique. I've had the pleasure of meeting you many times.

It's nice to see you, Mr. Van Laer.

Mr. Van Laer and I worked together on investigations relating to child sexual abuse and exploitation material. One of the reasons that I invited him here and wanted to hear from him is that we haven't heard from anybody yet who has told us what it's like to kick down a door or what metadata you look for when you're doing child sexual abuse investigations.

Mr. Van Laer, I'm going to focus my questions on you for the time being.

This bill focuses on metadata. Are you familiar with metadata in the context of child sexual abuse material cases and Internet luring cases? I assume you're aware of metadata and how it all works.

Mathias Van Laer: Yes.

Frank Caputo: This is something you've dealt with on the front lines. Is that right?

Mathias Van Laer: That's correct. There are layers of metadata, of course.

Frank Caputo: Yes.

You've dealt with cases that we may never have heard about, right up to the Amanda Todd case in B.C.

Mathias Van Laer: That's correct.

Frank Caputo: Does metadata assist in any way on child sexual abuse cases? Can you tell the committee how? We haven't heard anything like that so far.

Mathias Van Laer: That's correct.

First of all, metadata is quite broad, so there might be a need to make sure that we understand what exactly we are referring to when we say metadata. It's information captured by an electronic service provider insofar as every little bit of that information can be considered metadata.

Ultimately, the role of the police is not just to identify an Internet subscriber. An Internet subscriber is just the person who pays for the Internet connection. Our job, in order to satisfy prosecution, is to identify the person behind the keyboard. In order to do so, we need to dig into the content of what's happening on the Internet to identify the actual suspect user as opposed to simply a subscriber. The subscriber is a piece of the puzzle, and it leads our investigation into, hopefully, the user. We can't identify a user if we can't see their traces or identify them through some of their traces on the Internet, if that makes sense.

Frank Caputo: Let's say you get an IP address of a suspected child sexual abuser. What do you do from there?

Mathias Van Laer: Currently, what we are required to do from there is to draft a production order to get the subscriber's name and address. That process takes man-hours. It takes time to draft the production order, but then, insofar as the result of the production order, it is left to the Internet service provider to give us that result. It can take up to 30 days, if not more sometimes.

That's not the end of the road, though, obviously. Once we have the IP address identified to a subscriber, we then have an address. Once we have the address, we start to do our investigation into that address and into the residents of that address. Then, more often than not, it will lead to a search warrant. We will need to satisfy the courts and provide reasonable, probable grounds to believe an offence was committed within that residence and evidence exists within it. We will then go through that door, get and seize those computers and electronic devices, and look for the traces that led us to that door in the first place.

You have to remember that we don't get an IP address out of the blue. It's been pre-identified for us. It's been given to us by an electronic service provider that is self-reporting online criminal activity. They see it as criminal activity, they report it and then it lands on our desk, unsolicited. We receive those reports, which are provided to us voluntarily by the electronic service provider.

● (1815)

Frank Caputo: Once you have that information—you've kicked down the door, so to speak, and you've seized a number of things—what's your timeline, then, for investigation? What role might metadata play in identifying and arresting a child predator?

Mathias Van Laer: Digital forensics is going to have to take place. We are going to have to get those computers analyzed by digital forensics experts. Those are the people who are going to be able to see or say what was happening on the computer at certain dates and times. We will try to match the activity of the computer with the activity of the offender, and by doing so, that's how we can identify who's behind the keyboard.

The electronic service provider will collect the username, the IP address and pieces of information within the profile. That's what, sometimes, on more complex cases, may lead us to identify the same user utilizing different profiles because they can do that too. My colleagues who are also witnesses today are speaking of complex investigations. More often than not, we're looking at—never mind one offender—usually multiple profiles being used, and then we have to reconcile those different identities, online identities, to an actual, real one.

Frank Caputo: How long does all of this take?

Mathias Van Laer: The forensic analysis of a computer can take months. That's outside of the on-the-ground investigation. It depends on the resources and the capability. It depends on the content, the size of the computer equipment and the number of devices that were seized in order to conduct the investigation. There are multiple factors.

Frank Caputo: From there, then, is there a use for metadata in an ongoing investigation? I guess that's my question.

Mathias Van Laer: Absolutely. I think you were referring to the Amanda Todd case earlier. That's one of those cases where, if it weren't for the voluntary participation of a major electronic service provider, which was collecting that data already and co-operated with our investigation, thankfully—and I think they were in the right place to do so—we wouldn't ever have been able to identify a suspect overseas.

The Chair: Thank you, MP Caputo.

We have MP Sodhi for six minutes, please.

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

Thank you to all of our witnesses for appearing before the committee today.

I would like to ask Mayor Brown my first set of questions. First and foremost, I would like to wish one of the best mayors that Brampton has had a very happy birthday.

Mayor Brown, you have been one of the most more vocal municipal leaders calling for stronger lawful access tools for police services, particularly as Brampton and Peel region confront rising levels of enabled crime, including extortion and organized criminal activity predominantly targeting the South Asian community and their businesses.

Last year, in December of 2025, Brampton city council adopted a motion approving a letter to the federal and provincial governments calling for, among other measures, federal action on digital evidence access, a dedicated extortion and organized crime task force, victim support and community outreach funding, and the establishment of a formal intelligence-sharing framework across federal, provincial and municipal law enforcement.

Can you speak to what the measures in Bill C-22 will mean at a community level to our constituents in the city of Brampton?

Patrick Brown: Thank you for that question, MP Sodhi.

What I've heard from law enforcement is that this is an incredibly important tool that will make a world of difference.

Yesterday, we had a major police announcement by Chief Nish. There were 17 individuals arrested for violent extortions. I was told that the investigation took very difficult police work. You had police members who put themselves in harm's way to hold these international criminals to account. They told me that the investigation literally could have been done in two or three months, not eight months, and that there was a litany of victims in that period, which this legislation could have prevented.

It's not just extortions, MP Sodhi. I can tell you about some of the worst crimes in the region. This is a tool that could have prevented them. Let me give you one example that was shared with me by the Peel Regional Police. We had two victims of a recent cybercrime—a cryptocurrency scam—and the two innocent victims were defrauded of $1.6 million. This is a case where the lawful access provisions would have allowed them to get those responsible and to have them charged before this crime was successful.

For human trafficking and child exploitation to extortions, this is a tool that I think our police desperately need. When you hear chiefs of police and police unions across the country pleading for this help and saying that this is a tool they need, I can't comprehend why there would be such hesitation behind this. I was told very clearly by our chief of police, in whom I have a great level of confidence—I think he's one of the best chiefs in the country, and he was actually chief of the chiefs at one point—that this is balanced. It's carved out to focus on those crimes where there's a reasonable suspicion of a crime. There's not an overextension of where it could be applicable. For those who are sharing privacy concerns, I think you do not need to worry about your privacy being infringed if you're not committing criminal activities.

I'd ask this question: How about the right to privacy of victims? How about the right to not get your house shot up? How about the right to not have your children terrified?

Amandeep, you represent the Brampton riding. I'm sure you've heard countless concerns as well. I get calls from the victims who say, “What are you going to do, Mr. Mayor, to stand up for us?”

One of the things we've been doing is pleading with the Government of Canada to deliver updated lawful access legislation. I'm grateful that the government has done so. I know that our hard-working police officers are grateful that this hope and this help are on the horizon. I really hope that we don't see delays in the passage of this legislation.

● (1820)

Amandeep Sodhi: Thank you for your answer, Mayor Brown.

You've also been in contact with mayors and police chiefs across Canada and Peel region on this file, from Surrey to Edmonton to Hamilton. Is the position of your colleagues across different big cities on this bill broadly aligned with yours? In your view, how strong is the consensus among Canadian municipal leaders that Parliament needs to act?

Patrick Brown: I believe there's a strong consensus.

With organized crime, if they see a loophole.... Right now, they view a loophole in Canada that other Five Eyes countries have closed. We don't have lawful access for police. This is going to replicate itself across the country. It will mushroom. It may have started out in Surrey and Brampton, but we've heard of cases in Calgary, Edmonton and Winnipeg. I've had colleagues, other mayors across the country, call me and say the same terrifying incidents I've told them about are now happening in their communities.

Other gangs and organized criminal syndicates will commit these extortions and heinous criminal activities if they can get away with them. The lawful access legislation is a clear tool to police to make sure that they don't get away with them. Don't give a gift to organized crime. Don't dither and delay. Right now, it may be in 10 or 15 Canadian cities, but it will be in 100 Canadian cities in no time if we do not act. We've been too slow as it is, and that's why the police have been so united, clear and eloquent on the need for this legislation.

The Chair: You have 15 seconds.

Amandeep Sodhi: Thank you, Mayor Brown.

I have only 15 seconds, so I'll say thank you.

Patrick Brown: Thank you.

The Chair: I'm sorry.

[*Translation*]

I now give the floor to Mrs. DeBellefeuille for six minutes.

Claude DeBellefeuille: I would like to thank the witnesses very much for coming here today to appear before us.

Mr. Commissioner, I don’t know if you were connected to the meeting earlier, but representatives from the Barreau du Québec came to express their disagreement regarding the use of “reasonable grounds to suspect” rather than “reasonable grounds to believe”—the higher threshold—when issuing an order.

According to the president of the Quebec bar, including “reasonable grounds to suspect” in the bill does not respect the spirit of the Supreme Court’s decision. However, the Department of Justice and its minister claim the opposite.

Can you explain to me what difference it makes for investigators to use “reasonable grounds to suspect” rather than “reasonable grounds to believe” when issuing an order?

● (1825)

[*English*]

Commr Thomas Carrique: I can give you a very specific example in response to this important question.

Let's take a case where we have a missing person. That investigation is proceeding, and it gets to the point that we believe there may be foul play and the missing person may have been subjected to a homicide. We have a number of phone calls coming in to that individual's phone. These are the last known phone calls. That would not give us reasonable grounds, under the current legislation, to seek a production order. However, it would give us reasonable suspicion. That production order would only provide us with subscriber information, not content.

I think it is a very important, progressive step in our legislation to allow us to deal with the challenges of legislation and the complexities of technology, and to service the victims of crime much more efficiently and effectively.

[*Translation*]

Claude DeBellefeuille: If an amendment were proposed to remove the words “reasonable grounds to suspect” and replace them with “reasonable grounds to believe,” would that significantly hinder your investigative work?

Currently, you're still conducting effective investigations. You have reasonable grounds to believe.

Would that prevent you from doing your job well?

Would it be a major problem for you if that were removed from the bill?

[*English*]

Commr Thomas Carrique: The proposed changes to the threshold will not prevent us from doing our job. They will actually enable us to do our job better, more efficiently and in a more timely manner, and advance our investigations at a more rapid rate, while still requiring judicial oversight and judicial authorization.

As His Worship identified, in relation to finding the appropriate balance, I really believe having reasonable suspicion to obtain subscriber information as reasonable grounds to obtain content is the appropriate balance, given the modern context.

[*Translation*]

Claude DeBellefeuille: Commissioner, since the start of the study on this bill, we have known that Canada is the last of the Five Eyes countries to introduce a bill on legal access. In the other Five Eyes countries, such laws exist, in some cases for a very long time.

Do you have any statistics or reports that could establish a very close link between having a legal access law and a decrease in crime? In other words, do you have any documents or statistics showing that the legal access law in the United Kingdom, for example, has enabled that country to arrest more criminals and lower the crime rate?

Do you have any documentation on this? Is it available?

[*English*]

Commr Thomas Carrique: That's a great question. I don't have any documentation that would speak specifically to a reduction in crime rates or crime severity, but we have countless examples of investigations that have not been able to progress, including investigations into national security where there is a risk of terrorism, homicides and human trafficking. In other countries, these investigations would have progressed under an appropriate lawful access framework.

[*Translation*]

Claude DeBellefeuille: We are, after all, talking about a major change for Canada. We must therefore rely on an analysis of the statistics. That is what I am trying to document. I think Bill C-22 has its merits. It would give law enforcement better tools to fight criminals and crime. However, are we going too far or not far enough? We're trying to figure out where the line is.

I like to rely on data. Since such laws exist elsewhere in the Five Eyes countries, with which Canada likes to compare itself, have you been able to access information that would allow you to say that a law on lawful access will improve investigative performance, backed by data and results?

● (1830)

[*English*]

Commr Thomas Carrique: We could certainly determine whether or not there's specific data that can be used. There are very specific, compelling examples of when people have been victimized in Canada, when victimization has been prevented in other countries, when complex investigations have been solved in other countries and when we are just not able to be meaningful participants in international and transnational organized crime investigations. We're happy to share any of these examples that would help you make an informed decision.

[*Translation*]

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

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

[*English*]

Frank Caputo: I believe it's MP Lloyd.

[*Translation*]

The Chair: Mr. Lloyd, you have the floor for five minutes.

[*English*]

Dane Lloyd: Thank you, Mr. Chair.

Thank you to the witnesses.

Mayor Brown, happy birthday.

Something you said really struck me. You said if people are concerned about their privacy, don't commit a crime. Their privacy won't be abridged. However, something we've learned with this legislation—we saw it with the Salt Typhoon hacks in the United States—is that if we create the ability for ministerial orders to infringe upon the integrity of encryption systems, we could be creating back doors that hackers could be using to go after the information of innocent, law-abiding Canadian people.

My question for you, Mayor Brown, is this: Would you still support this legislation if you knew we were creating a vulnerability that could result in your own personal information and your own private messages being hacked and used by extortionists?

Patrick Brown: I have confidence that the system set up and used by law enforcement in other Five Eyes countries can be replicated here.

Frankly, we have too many preventable victims. I certainly support the legislation. If there are additional protections to ensure that there isn't a capacity to be hacked, I would welcome them, but if tech companies can prevent that through their own cybersecurity measures in other countries, like the U.K. and the U.S., it's bewildering to me that they wouldn't have the same capacity to do that in Canada.

Dane Lloyd: That's precisely my concern, Mayor Brown. This legislation is actually hindering their ability to create those security.... They could, potentially, be lowering their security safeguards.

I'm going to move on to Commissioner Carrique.

This is clearly important legislation. I could feel the passion. I talked to law enforcement, and clearly, we need to do something about this.

Is this legislation so important to you that you would support amendments to ensure that Canadians and industry can have confidence that encryption will not be violated under this legislation? Would you support those amendments to make that very clear?

Commr Thomas Carrique: I would certainly support amendments to ensure that there is clarity around not compromising the integrity of systems, and I believe there's an opportunity to do that in the creation of the regulations.

Let's be honest. We have major tech that has completely redefined the world as we know it. It has created such innovation and progress. There has to be a way, with the hundreds of billions of dollars it's generating every year, to safeguard the encryption of law-abiding Canadians, while allowing us access to criminals who are victimizing Canadians.

Dane Lloyd: Commissioner, are you saying to this committee that law enforcement needs the power to break encryption? Is that what you're saying to the committee today?

Commr Thomas Carrique: I am absolutely saying we need judicial authorization to access encrypted data, and we have that lawful access today. The current legislation provides us judicial authorization, when granted by a provincial superior court judge, to gain access to private communications. What we don't have is the keys to encryption, so we have to use on-device investigative techniques.

We have the judicial authorization, but we don't have the means or mechanism, and there's a big difference.

Dane Lloyd: Thank you.

Maybe this is a question for Mr. Van Laer, but it's also for Commissioner Carrique.

In talking to the integrated child exploitation teams in Alberta in the wake of the Bykovets Supreme Court decision, it became a nightmare to write warrants and production orders. If we don't know if there's a reasonable expectation of privacy around IP addresses, it seems to me that part 1 actually provides the appropriate remedy to allow law enforcement to speed up their ability to get these warrants written so that they can go after the telecom or ESPs that have the information.

Is that correct? Is part 1 largely what's needed to speed up these investigations, Commissioner?

Commr Thomas Carrique: Yes, it is. It is a good portion of what is needed to speed up these investigations, and I appreciate you highlighting it, sir.

● (1835)

Dane Lloyd: Mr. Van Laer.

Mathias Van Laer: I would agree that the issue we face.... We don't really have so many issues with this new court decision with regard to getting our judicial authorization. We have to understand where the IP comes from in the first place, so if the IP is....

I'm sorry. Go ahead.

Dane Lloyd: Commissioner Carrique, the Privacy Commissioner brought forward some very good recommendations, in my opinion. He said instead of having a one-year mandatory metadata retention period, we have a necessary and proportionate test. Is it necessary and proportionate?

Would you support that amendment? Do you think that might be stronger and give Canadians some peace of mind?

Commr Thomas Carrique: I'm not sure how that would relate if the metadata was not retained for one year. We may not realize that it's reasonable and necessary until that data is no longer available. I'd have to learn more about what that recommendation is to be able to provide you with an informed response.

Dane Lloyd: I appreciate it. Thank you.

The Chair: Thank you, MP Lloyd.

MP Sidhu, go ahead for five minutes, please.

Sonia Sidhu (Brampton South, Lib.): Thank you, Chair.

Thank you, committee members, for giving me the time.

Thank you, Mayor Brown. Happy birthday to our hard-working mayor.

Mayor Brown, you have publicly stated that the police and border agents need stronger tools, and they need faster and more effective access to digital subscriber and transmission data to identify suspects before an attack occurs. We know you are a long-standing advocate for increased supports and digital screening tools for our law enforcement officers, and for the safety and security of Brampton. Our communities are terrified by extortions, and there are other crimes, too.

How do you think Bill C-22, the lawful access for law enforcement legislation, can give modernized tools to law enforcement and police agencies and also build trust in the community?

Patrick Brown: The last part of that question, about trust, is so important. Right now, there is a sense of hopelessness because so many of these extortion investigations have gone cold. I hear again and again from law enforcement that if we had lawful access, they would be able to chase this one down, but it goes cold.

Let me give you an illustration of what I mean, MP Sidhu. If the Peel police observed a suspect.... This is from a senior officer who shared this with me about why he needs this legislation. He said if you were to observe a suspect, after a crime, speaking on a cellphone on the video camera, the police could write a production order for a cell tower site. Right now, that order would take upwards of three, four or five weeks, or maybe 45 days, and then all of the key evidence would be lost. Evidence would be lost. Video would be lost. More crimes would potentially be committed, and the criminals would evade justice.

To give another illustration, one of the investigations we had recently was successful because they had lawful access in the U.S. One of the criminals was operating out of the U.S. and they were able to nab him.

Canadian law enforcement shouldn't have to depend on other countries to do their job. They should have the same modern tools that other countries with similar charter protections and similar laws have. If other countries found that balance, I know Canada can. I believe this is a balanced approach that our hard-working police desperately need.

Sonia Sidhu: Thank you.

We know that criminal activities are increasingly moving into online spaces, making it harder for traditional policing methods to keep up.

Do you think it will provide more tools to combat online crime as well?

Patrick Brown: Yes, 100%. Online crime has become the new digital warfare. Unfortunately, criminal organizations are very sophisticated when it comes to technology. If they view a loophole in Canada, they will take advantage of it.

This is an important tool in preventing cybercrime as well. There are many aspects to this bill, all of which have been asked for by law enforcement. They're the ones on the front lines. As MP Caputo said, they're the ones banging doors down, chasing down evidence. If the people doing that very challenging work—the law enforcement, who put their necks on the line—say that this is the tool they need, I have confidence in our men and women in law enforcement and that, as this is a tool that has been successful in other countries, it will be successful here.

● (1840)

Sonia Sidhu: Thank you.

I saw you join Chief Nish yesterday in a press conference about the 17 individuals with extortion-related offences. We all saw the press conference. You told us in your testimony that this investigation spanned eight months, but that could potentially have been reduced if this modernized tool was given to the police before.

Do you think seniors, who are often targeted by scams and financial exploitation, could benefit from this?

Patrick Brown: Certainly.

There are seniors who are being taken advantage of through cybercrimes, although you may not hear about them as much as the extortions that are all over the news in Peel region. However, for crimes like that as well, I think it would be an important tool for law enforcement.

One of the people testifying before this committee in the next segment is Deputy Chief Nick Milinovich. I believe he's one of the smartest minds in the country when it comes to technology and law enforcement. I think you'll really enjoy asking him technical questions about why this legislation is so important. He can explain very specifically why it would help in those specific instances.

Sonia Sidhu: Mr. Chair, do I have any more time?

The Chair: I'm sorry. No, you don't have any more time.

Sonia Sidhu: I just want to thank you, Mayor Brown, for joining us today and for your continued focus on public safety, because it's very important for our city of Brampton.

Thank you.

The Chair: Thank you, Ms. Sidhu.

Ms. DeBellefeuille, you have two and a half minutes.

[*Translation*]

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

Commissioner, I would like to discuss the issue of retaining metadata for one year.

We have raised this issue with department officials. They set the retention period at one year in what appears to be a rather arbitrary manner. In Australia, it is two years. I have heard that in the United States, no specific period is set.

What does a one-year period mean to you, as an investigator?

We have received recommendations to set this at 90 days or three months, for example, and to make these periods renewable upon request, rather than retaining all Canadians' metadata for a year.

If we reduced this period, under certain conditions, and allowed you to request the data again, could you live with that? I don't really understand the importance of having a one-year retention period.

What is your perspective on this as a police officer and investigator?

[*English*]

Commr Thomas Carrique: Thank you.

I do think that one year is a reasonable time period, given the length of time that it takes to progress through the necessary investigative steps on any serious or complex criminal investigation. Right now, the Criminal Code does provide us with the ability to obtain preservation orders that limit retaining known data to 90 days. However, 90 days is not enough time for us to conclude an investigation. We would find ourselves not knowing what we needed to know before that metadata was no longer available to us.

As I understand the way the legislation has been written, there is an opportunity to review the legislation at a later date. At that time, it may be appropriate to determine whether the time frame that has been provided—under one year—in the current version is sufficient.

[*Translation*]

Claude DeBellefeuille: Commissioner, there are still many witnesses who say that one year is too long. Some believe we should limit the data retention period and require more renewals through the courts, for example.

If we keep the metadata of all Canadians, that's still a lot of data, and it opens the door for criminals. They could then steal that data. That's what the companies are telling us, too.

What do you think?

[*English*]

Commr Thomas Carrique: Certainly, I have no knowledge of how that would compromise systems and make people more vulnerable to criminals. My understanding of the metadata that we're looking to retain for a year is that it's very specific as it relates to date, time, duration and origin of transmission. It is not content like emails or browser histories or social media activities. Even for that basic metadata, for the bare minimum that could assist in complex investigations, we would still require judicial authorization.

From a police perspective, I do believe it is a reasonable time frame.

● (1845)

[*Translation*]

The Chair: Thank you, Mr. Carrique.

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

[*English*]

Frank Caputo: I'd like to build on what Madame DeBellefeuille just said, Mr. Van Laer, and get your opinion on metadata and timelines. I feel that one thing we are lacking as a committee is piecing together how metadata assists investigations.

Are you following me here so far?

Mathias Van Laer: I think so.

Frank Caputo: Can you comment on that? In what situations would you need metadata for only 30 days, 60 days, 90 days or one year? Can you envision any sort of scenario here? The bill here says that you have to keep metadata for a year. That is an arbitrary number. Why is it a year?

I guess what I'm trying to figure out is this: Based on your investigative experience over the course of thousands of investigations, what is your experience as to how long data should be kept?

Mathias Van Laer: It's a bit of a difficult question to answer in the sense that if investigations were not able to be pursued because the data had expired, for instance, we wouldn't know where or how far we could have gone had the data been available in the first place.

Frank Caputo: How often are you missing data in your investigations, would you say?

Mathias Van Laer: Unfortunately, because of a number of factors, it happens quite a bit at the moment due to a number of delays in the process and the time it takes sometimes for a simple investigation to even be initiated. At the start, we need to be able to have access to subscriber information, for instance. If we have an electronic service provider or an Internet service provider that is not compelled to keep those records for any length of time, then we can be basically shut down before the investigation even starts.

Frank Caputo: Can you give a timeline? Based on your experience, is there a number you can assign to say, “Look, right now, electronic service providers keep this data for 90 days, and that frequently shuts us out of our investigations”?

Mathias Van Laer: I don't know that there's an actual number I can provide other than, as you mentioned, my experience. I've had the unfortunate scenario of having to close investigations because the data had expired. We have to remember where the source is coming from. By the time information that comes from other countries trickles down to Canadian authorities, never mind to provincial jurisdictions and then to municipal jurisdictions, that time can expire very quickly.

I'm not here to give you a number. I'm just here to explain the reality that this timeline is of the essence.

Frank Caputo: Okay.

Commissioner Carrique, you have spoken at length, and very passionately, about the necessity for this bill. As somebody who comes from a prosecutorial background, I understand that. I think one of the main things I'd like to ask you about...and Mayor Brown is free to weigh in on this as well. This is important legislation, but it's equally important that we get it right—for instance, on the “reasonable grounds to suspect” versus the “reasonable grounds to believe”. Would you support the fact that this is complicated stuff?

We can't even agree on a number, for instance, for retaining metadata. At some point, we have to delve into this and get it absolutely right. I don't think there's much room for error here. I feel that the process has been rushed on this. Mayor Brown used the word “dither”. In my life, I have looked at the ceiling at night in investigations where we could not put the person behind the computer. It sucks. At the same time, we as parliamentarians have to make sure we get it right.

What do the two of you say to that?

Commr Thomas Carrique: MP Caputo, I know that if anyone understands, it's you, as you have been a prosecutor. It is important to get this right. I also think we can't waste time diving into things that are really not important or not overly relevant, like debating timelines of three months, six months, nine months or 12 months. We have to start somewhere.

I can tell you that as a young detective constable in 1996, in a group that was working under Criminal Intelligence Service Ontario, I brought this matter forward to say that we were being hindered by the advancement of technology and outdated legislation. Thirty years later, we've seen no substantive change. The first of many resolutions from the CACP was issued and shared with the federal government in 2002. There has been no substantive change.

I guess my question would be, how long does it take to get it right and how many more victims are harmed in the process?

● (1850)

Frank Caputo: Go ahead.

Patrick Brown: I would just add that I believe the reason this bill is in its current form is that there was concern that the strong borders act, which was the first iteration of this, went too far. They wanted a more targeted, carved-out focus on criminality. I believe this bill is that attempt to pause and put forward new legislation targeted toward criminality. At least that's the feedback I've heard from the local Peel police, who have been consulted on the legislation.

The Chair: I'm sorry to interrupt, MP Caputo and everyone else.

Let me turn to MP Ramsay for five minutes, please.

[*Translation*]

Jacques Ramsay: First, I want to thank the three witnesses.

They were very eloquent. I had several questions, and they answered them. However, I would like to return to one of those questions to clarify things.

There is a sense that we are rushing things and that everything is a bit improvised. I think you have all clearly demonstrated that the provisions of the bill are quite well thought out and that they address very specific needs.

People often try to give the impression that the government has embarked on a hunt for all kinds of information regarding metadata. However, I think it is important to clarify one thing. To my knowledge, the metadata covered by the bill is as follows:

[*English*]

Internet transmission data, tower signalling data, signalling data for VOIP calls and vehicle manufacturer telemetry data.

[*Translation*]

That is all there is to it. It is specific. I think that instead of arguing, we should acknowledge that Bill C-22 actually clarifies the scope of the data and prevents a witch hunt.

I would like to hear your opinion on this, Commissioner.

[*English*]

Commr Thomas Carrique: Thank you very much, member of Parliament. I would be happy to weigh in on this.

I agree with you. It is very finite. In my comments, I indicated that it be the bare minimum of information that could assist investigations. There are no fishing trips or fishing expeditions here. We would still require judicial authorization to access any of that metadata. I agree with your comments wholeheartedly.

[*Translation*]

Jacques Ramsay: I am very pleased to hear that.

One of the witnesses from the Barreau du Québec even seemed to claim that with an IP address, one could access our dreams. That’s a bit of a stretch. It’s a bit of nonsense. The IP address remains basic information that will allow police, with a warrant, to go and get the information they need.

The other point we discussed is the famous three-month period, which might be insufficient. What I gathered from all three of your testimonies is that investigations often begin after crimes have already been committed, and we can’t know in advance what information we’ll need. So, we can’t say we’ll just keep a specific piece of information because that’s all we’ll need. That’s not how it works.

Mr. Van Laer, what are your thoughts on this?

Mathias Van Laer: Thank you for your question.

I agree with you.

To answer your first question, I’d like to comment on the IP address, if I may. You’re absolutely right: We don’t have access to everyone’s dreams through an IP address. So, I’m glad that this has been taken into account as a factor. It’s important that the people here, around the table, can develop laws based on real activities or processes—that is, things that are actually possible. It’s impossible for anyone to identify someone based on an IP address without going through a judicial process. So, that’s important.

To answer your second question, I would say yes.

I hope that answers your questions.

Jacques Ramsay: My third question concerns the reason to “believe” as opposed to the reason to “suspect”.

It is clear that, in this case, we are talking about a reason to suspect someone, because we are seeking information that will not serve as evidence per se. An IP address, or a telemetric address, is not evidence to charge someone or find them guilty. So that is why the legislature wanted a significant and recognized legal standard, which is the reason to “suspect” rather than the reason to “believe.”

Commissioner Carrique, what do you have to say about this?

● (1855)

[*English*]

Commr Thomas Carrique: I agree. Reasonable grounds to suspect is the appropriate standard, as I've stated earlier.

Let's compare it to a previous time when we were operating under landline phone lines. You could go to a phone book, look up a name and get a phone number—not only a phone number but the address of an individual. There was a lot more private information available in a standard phone book of years gone by, as opposed to requiring reasonable grounds to suspect a crime has been committed simply to get an IP address to commence an investigation, which will then require more substantive evidence before you have reasonable grounds to lay a charge.

[*Translation*]

The Chair: Thank you very much for these remarks, Mr. Ramsay. This brings us to the end of this important hour of discussion.

We thank the three witnesses for their time and the quality of their remarks. We wish them a good rest of the day.

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

● (1855)

_____(Pause)_____

● (1900)

The Chair: We are resuming the meeting.

I welcome the members back and greet all the witnesses.

We shall resume the meeting by welcoming our distinguished guests: the Canadian Telecommunications Association, represented by Mr. Eric Smith; the Ontario Child Sexual Exploitation Investigators Association, represented by Andrew Ullock and Lisa Henderson, both participating via video conference; the Peel Regional Police, represented by Mr. Nick Milinovich; and Murray Rankin, a highly esteemed colleague whom we have missed for a very long time and whom we are fortunate to see again today among us in person.

We will begin by hearing a five-minute statement from each person.

Mr. Smith, you have the floor.

● (1905)

[*English*]

Eric Smith (Senior Vice-President, Canadian Telecommunications Association): Thank you, Chair and members of the committee, for the opportunity to appear before you today on behalf of the Canadian Telecommunications Association.

Our association is dedicated to building a better future for Canadians through connectivity. Our members include service providers, manufacturers and other organizations that invest in, build, maintain and operate Canada's world-class telecommunications networks.

Having listened to the discussions before this committee, I will say it is clear that there is broad agreement on two important principles. First, Canadians' privacy rights must be protected. Second, law enforcement and national security agencies must have the ability to access information through lawful processes to support legitimate investigations and protect public safety.

The central question, therefore, is not whether these objectives matter: It's how to appropriately balance them. That balance is critically important because Canadians use digital services every day with the expectation that their personal information will be handled securely and that any access to that information will occur within a clear, proportionate and accountable legal framework.

We appreciate the efforts of government in consulting with stakeholders and making Bill C-22 an improvement over the earlier proposals in Bill C-2. To be clear, we are not against the bill. However, we have remaining concerns, which are set out in a written brief that has been provided to the committee. I'll touch on three of them.

One item that hasn't been mentioned before deals with part 1 and the requirement that confirmation of service demands must be responded to in as little as 24 hours. While most service providers have processes in place to deal with urgent requests from law enforcement, treating all confirmation of service demands with the same level of urgency and a 24-hour turnaround time is impractical and unrealistic.

The number of requests, the complexity of searches and the fact that not all service providers have staff available on a 24-7 basis make an across the board 24-hour response time near impossible to facilitate. A more workable response time would be no less than three business days, which would be suitable for most situations and would not prevent service providers from responding to truly urgent requests in a shorter period, as they do today.

The second concern is the requirement to retain broad categories of metadata for as long as one year. You've already heard from other witnesses about the privacy concerns this requirement raises. We are also concerned about the security risks as well as the lack of guardrails around the use of metadata. The metadata provisions of Bill C-22 should either be removed or substantially restricted, both in retention time and purpose.

Finally, there is the issue of reimbursement for the substantial cost of providing lawful access services. These are state-mandated tools and services created for the exclusive use of law enforcement and security agencies and are not part of normal commercial operations.

In a previous government consultation on lawful access, law enforcement agencies submitted that communication service providers "should be able to recover reasonable costs incurred in providing court-ordered assistance".

Likewise, the lawful access advisory committee established by the RCMP and CSIS has as one of its key principles a commitment to a cost-neutral and fair compensation model. Again I will quote:

> The lawful access community acknowledges that [communication service providers] are private or semi-private companies and deserve fair compensation for the effort required to develop, maintain, and operate capabilities that is not part of their normal business processes.

These economic realities are recognized in other jurisdictions, such as the U.K., which reimburses telecommunication providers for both capital and operational costs associated with the creation of intercepting capabilities and the production of communications data. This concept should be included in Bill C-22.

Reimbursing service providers reflects the philosophy underpinning U.K. law that while private companies have a statutory duty to assist with the implementation of warrants, they should not be expected to act as an uncompensated arm of the state. Government funding also helps ensure market fairness and competitiveness, mitigates financial impacts on smaller businesses, provides oversight over the quality, standards and security of intercept capabilities, and prevents citizens from facing increased monthly bills to pay for law enforcement investigation infrastructure.

In closing, we understand the need to update Canada's lawful access framework. With targeted refinements, Bill C-22 can provide a framework that balances the interests of privacy and public safety, and that is proportionate, accountable and does not pass the costs to Canadian consumers.

Thank you. I'd be pleased to answer your questions.

[*Translation*]

The Chair: Thank you, Mr. Smith.

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

● (1910)

[*English*]

Andrew Ullock (Board Chair, Ontario Child Sexual Exploitation Investigators Association): Good evening.

Thank you for giving us the opportunity to share with you the perspective of the Ontario Child Sexual Exploitation Investigators Association, or OCSEIA, on Bill C-22. OCSEIA is comprised of police officers, former Crown prosecutors and members of the private sector who work together to advocate for those who work to rescue children from online child sex offenders.

My name is Andrew Ullock, and I volunteer as the chairman of the board for OCSEIA. I am an officer with 28 years of experience, 14 of which was in the field of online child exploitation. I have worked both as an investigator and a supervisor of officers in this field.

Joining me is fellow OCSEIA board member, Lisa Henderson, who recently retired after working for over 30 years as a Crown prosecutor. Since the early 2000s until her retirement, Lisa worked both as the chair of the Attorney General's task force on Internet crimes against children and also as the provincial Crown coordinator for Ontario's provincial strategy to combat Internet crimes against children.

The law must create a proper balance between protecting privacy and protecting the public from crime. As technology continues to evolve, the challenge of striking this balance becomes more and more complex. One of the bedrock foundations of criminal law in Canada is that the burden of proof falls to the state, exercised through its agents in law enforcement. The state must establish beyond a reasonable doubt that an individual is guilty of a crime, an essential safeguard that cannot be compromised. That being the case, if law enforcement is tasked with the burden of meeting this necessarily high threshold, then the law should have within it reasonable tools that make it possible for the police to accomplish this objective.

Since the creation of the Internet, there has been very little change in statutory law to regulate the manner in which police obtain evidence of criminal offences, be it online or in computer data stored on devices. Without updates from Parliament, the courts are forced to adapt by filling the legal gap with a patchwork of decisions that can be confusing, inconsistent and redundant. This patchwork amounts to what OCSEIA calls legal inflation, where the number of steps and authorizations that police must go through to complete an investigation increases over time but never decreases.

Time is a finite resource for law enforcement. There are simply only so many hours a single officer can work in a given year. As the amount of time required to complete an investigation increases, the number of investigations that police can complete simultaneously decreases. The objective of privacy laws should not be to create redundant obstacles or barriers that are impossible for the police to overcome. Sensible limits on the investigative powers of police protect the privacy and dignity of citizens; insensible ones protect crime.

Bill C-22 has inspired a lot of discussion regarding the privacy rights of Canadians. OCSEIA agrees that this is an important debate and appreciates the contributions made by privacy advocates. However, on the topic of privacy, OCSEIA wants to ensure that the discussion is a complete one that considers all facets of this issue.

Behind each statistic or police report regarding online child exploitation is a real child who has suffered immense abuse at the hands of a predator. These children are equally entitled to have their privacy considered in this debate, since it is their privacy that is violated in perpetuity in the most horrendous way imaginable. Once an offender creates and then shares an exploitive image of a child, it becomes a permanent part of the Internet. From that point forward, that child's privacy rights get trampled upon each time a new offender consumes or shares that image.

The best way we as a society can respond to these violations of privacy is to find and hold accountable those who thrive on the abuse of children. To do that, law enforcement needs the right tools. OCSEIA believes that there are a lot of reasonable tools that can be brought about to accomplish this.

Law enforcement in Canada should not have to obtain a mutual legal assistance treaty order instead of a production order to obtain content data from online service providers who are physically present in Canada, just because they are international companies.

Law enforcement should not have to obtain a second redundant search warrant to analyze a computer device simply because it was seized from a person's hand or pocket during the execution of a residential search warrant that already authorized the seizure and analysis of any device found in that place.

Law enforcement should not have to obtain prior judicial authorization to seize an IP address that is being broadcast in plain view to millions of other users over a peer-to-peer file-sharing network.

Law enforcement should have the ability, through prior judicial authorization, to obtain Internet subscriber information for longer than 30 days after an offender has exploited a child, thereby allowing them to find that offender and, in some cases, rescue a child being abused.

To be reasonable, investigative authorities for law enforcement must not unreasonably intrude on the privacy of citizens. On that, we can all agree. However, they must also be capable of accomplishing their intended purpose. It is not reasonable to expect law enforcement to protect society from crime a quarter of the way through the 21st century using search and seizure laws drafted in the 19th and 20th centuries.

● (1915)

OCSEIA believes that our input and recommendations will go a long way in assisting Parliament to find the right balance.

We are happy to take any of the committee's questions.

The Chair: Thank you, Mr. Ullock.

Mr. Milinovich, you have the floor for five minutes, please.

Deputy Chief Nick Milinovich (Deputy Chief of Police, Peel Regional Police): Chair and members of the committee, thank you for allowing me the opportunity to speak about Bill C-22, an act respecting lawful access. This discussion sits at the intersection of two priorities that Canadians care very deeply about—public safety and privacy interests. As police leaders, we support both.

Crime has evolved significantly over the last decade. Organized crime groups, extortionists, human traffickers, fraud networks and—as we just heard—child exploitation offenders operate primarily through digital platforms, whereas many investigative authorities were developed for a much different technological environment.

The objective of Bill C-22, from our perspective, is not to weaken privacy protections or to expand unchecked government authority. It is to ensure that investigators can continue to lawfully obtain critical evidence in serious criminal investigations while remaining subject to judicial oversight, legal thresholds, accountability and charter protections.

Today, I would like to share the perspective from our front line, our investigators and our community, which has been affected deeply by crime. They have a vested interest in this topic. On their behalf, I urge the swift passage of Bill C-22, the lawful access act.

Our current investigative laws were built for a pre-digital world. Today, criminals are actively taking advantage of that lag in high-growth regions and diverse regions like Mississauga and Brampton. We are seeing tech-facilitated crime move at an entirely unprecedented rate.

Our teams are hitting systemic and artificial walls. We are watching active threats disappear into digital shadows, simply because our legal framework forces us to investigate 2026 digital sophistication with outdated analog tools.

Yesterday, our service announced the outcomes of one of the largest extortion investigations in our community. It started with a threat that was delivered digitally from an encrypted platform in November 2025. If Bill C-22 had been in place at the time, it would have resulted in a more effective and efficient investigation and the closure of those extortion threats.

In Peel region—and in Canada—police are combatting a highly disruptive rise in extortion rackets, human trafficking, child exploitation and a variety of other transnational crimes. Almost every single one of these cases shares an identical pattern. It starts with digital communication, an encrypted message and an online profile or anonymous IP address, before escalating into real-world violence on our streets and impacts for our community.

Right now, when a digital tip comes in, identifying the telecommunications carrier or provider that hosts that suspicious account can take weeks of bureaucratic back-and- forth. By the time we navigate that maze, the trail can be cold, data is deleted and evidence is lost. The reality is that criminals are continuing their activities and continuing to prey upon our communities.

I believe that Bill C-22 introduces the necessary measures to radically shorten our investigative timelines. It allows us to narrow down suspects and stop a series of criminal activities before they turn violent. It will allow us to prevent victimization and crime in our communities.

As law enforcement professionals, we swear an oath to uphold the Canadian Charter of Rights and Freedoms. We do not want arbitrary surveillance capabilities in our community. Privacy and public safety must and can coexist, and I believe Bill C-22 strikes that balance.

As I mentioned, we recently arrested 17 people who were targeting our South Asian business community. This investigation, again, has taken seven months to date, and it is continuing. During that time, we believe that this group was responsible for firing over 320 rounds in our community. That's more than half of the rounds fired from illegal firearms in our community this year.

We are very pleased with the results, but as I mentioned, I believe it could have been quicker and more effective, and we could have prevented more victims of crime.

● (1920)

This is the case, again, for extortion investigations, but it's also been the case for homicides, national security investigations, human trafficking and, as we've heard, child exploitation, as well as a variety of other transnational crimes we are beginning to experience very locally in our communities.

Timely access to digital evidence has to be non-negotiable if we want to better locate victims and prevent community harm. I believe Bill C-22 provides the precise, transparent and judicially overseen tools we need to better do our jobs. We ask for your support to pass this vital legislation.

Thank you. I'd be happy to answer any questions.

The Chair: Thank you, Mr. Milinovich.

[*Translation*]

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

Hon. Murray Rankin (Barristor and Solicitor, As an Individual): Thank you, Mr. Chair.

Members of the committee, thank you very much for inviting me to appear today. I'm pleased to be here to discuss Bill C-22.

This is an important, complex and sensitive piece of legislation. It touches on public safety, privacy, cybersecurity, the Canadian Charter of Rights and Freedoms, and the actual ability of police officers and members of the Canadian Security Intelligence Service to do their jobs in a digital world.

This debate is not merely technical; it's a societal debate. How do we protect Canadians from child sexual exploitation, fraud, extortion, terrorism and espionage, while safeguarding the fundamental rights that define our democracy? In my view, these objectives are not contradictory; they're complementary. Government access to information must be lawful, necessary, proportionate, clearly authorized and subject to effective accountability.

I served as the first chair of the National Security and Intelligence Review Agency, and that experience left a deep impression on me. It taught me two things. First, security and law enforcement agencies need modern tools. Second, these tools must be governed by clear legislation, an independent oversight body and Parliament.

[*English*]

That is why I strongly support the need for a lawful access bill. The digital world has changed the nature of investigations. Criminals, hostile states and sophisticated networks use technologies that simply didn't exist when many of our investigative tools were designed. Canada desperately needs a modern legal framework, but it must be a Canadian-made framework. It has to be compliant with our charter, privacy-protective, technologically realistic and subject to meaningful oversight.

I was pleased to assist in the consultation process following Bill C-2. I met separately with stakeholders from law enforcement, national security, industry, civil society, academia and privacy communities. In my view, bringing them together in one room was a very positive experience. People disagreed, sometimes strongly, but the process was meaningful. I believe my report reflects the range of perspectives accurately.

I was also pleased that the vast majority of my recommendations found their way into Bill C-22. The bill is now stand-alone. The information demand has been narrowed and reframed as a confirmation of service demand. The bill includes greater attention to oversight, transparency, cybersecurity and parliamentary review. That does not mean the bill is perfect. No bill ever is. The minister has said he is open to amendments, and I take that seriously. As a former member of Parliament, I have great respect for the work of parliamentary committees like this one. This is where legislation can be improved and made more durable.

In my respectful view, the task before you is not to choose between privacy and public safety; it's to insist on both. The bill should preserve operational effectiveness while protecting privacy, charter values and cybersecurity. It should protect privileged, medical and highly sensitive information. It should ensure that any new powers are used properly, by properly trained officials, and reviewed after a reasonable period.

I would particularly encourage this committee to focus on five issues: the clarity of the confirmation of service demand, the definition of systemic vulnerability, the role of the intelligence commissioner and NSIRA, transparency and annual reporting, and a mandatory parliamentary review after three years.

Finally, I believe the purpose of this legislation should be made plain. State access to information for investigative purposes must be lawful, necessary, proportionate and subject to effective authorization and accountability, consistent with the charter and Canada's privacy laws.

Thank you again for inviting me, Mr. Chairman. I look forward to your questions.

● (1925)

[*Translation*]

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

Ms. Kirkland, the floor is yours for six minutes.

[*English*]

Rhonda Kirkland: Thank you, Mr. Chair.

Thank you all for being here.

I would be remiss to not mention again that I feel like I'm drinking from a fire hose, as the phrase goes. There's so much information here. There are five different people. I would love to spend all of my time delving into each one of their opening testimonies, but frankly, we don't have the time to do that, which is unfortunate.

I know that you all appreciate the role of members of the opposition, specifically you, Mr. Rankin. I appreciate your being here. You were an opposition MP for a number of years, so you understand that sometimes in opposition it looks like you're just opposing when that's not the case. Those of us who are looking very closely at this want to get this right. I'm nervous that the role of MPs in opposition is being negated a little bit when we rush through legislation. Words like “dither” were used earlier, which I didn't appreciate, simply because we want to look at this in depth. It deserves to be done right.

In 2012, a Conservative government tried to do this and ended up having to back off because the Liberal public safety critic at the time had a real problem with it. This bill actually takes things a little further.

I got into a bit of a preamble, but there's so much I really want to dig into. I know I can ask you all privately, but that wouldn't allow Canadians and Quebecers to hear what they need to hear openly and in public.

Mr. Rankin, you mentioned the process you went through and the round tables. I'm really happy to see you here. I'm happy we did get a version of the report. It might have been redacted somewhat, but at least it's something. This was something I asked for, so I'm very happy to see it here.

How long was the process that you spent on this? If you were to put it in hours, would you be able to give that number, approximately?

Hon. Murray Rankin: Thank you so much, MP Kirkland.

Thank you for the reference to being an opposition politician and for the recognition that it was the role I played here. I respect very much what you said about not simply opposing but about an effort to make things right. Getting it right is critically important for a bill like this.

I think we have an opportunity, and it starts with the 2025 NSICOP report. All parties came together in that report to understand the need for lawful access. It was a very thoughtful report. That gives us an opening.

Some people say this is the seventh time we've tried. Some people say it's the ninth time. You referenced one of the Conservative efforts. It's just one of many. It's overdue. You've heard from all sorts of witnesses. I've listened to them talk about the fact that they're handicapped by not having the tools they need in a digital world.

Rhonda Kirkland: I'm sorry. I don't want to interrupt, but my time is limited.

You mentioned the round tables. Do you know how long you spent...?

Hon. Murray Rankin: I was coming to that. I would think it was between 20 and 30 hours. I'm just guessing.

● (1930)

Rhonda Kirkland: It was between 20 and 30 hours.

Hon. Murray Rankin: We had separate meetings with each stakeholder group and then a group meeting.

Rhonda Kirkland: That's good. In this process, our committee is getting between eight and 10 hours. I would love to get 20 to 30 hours to fully understand this.

I know you'll probably revert to some of the things you were saying. Were there any major concerns raised during the consultations that you believe could have been better addressed or that were not fully addressed or incorporated into the final legislation?

Hon. Murray Rankin: The issue Mr. Smith just raised about compensation came up, and it's reflected in the bill as regards non-core providers explicitly. “Appropriate” compensation are the words used. With regard to the core providers, it's left open. That's something that might well be considered.

I've said elsewhere that metadata wasn't the subject of a great deal of our concern. Data preservation was obviously an important feature, but we didn't delve into that in great detail.

Those would be the two that come to mind.

Rhonda Kirkland: It's interesting that you bring that up, because those are some of the things we've had the most questions and testimony on in this committee. There's a reason for that. When there's not enough information, we have more questions. I appreciate your bringing that up.

I know you said elsewhere that the one-year retention period was never brought up. I think that's what concerns Canadians the most, because we're not talking about just the bad guys' metadata. We're talking about everyone's metadata.

Can you comment on that at all, or do you want to comment on that at all?

Hon. Murray Rankin: I know the committee understands well the difference between content and metadata, with metadata being about access to when and where a call took place, who was on it and so on. In the past and, I guess, currently, the retention period for metadata has varied dramatically, so I think it's interesting and important that we put our hands around a time frame—the bill calls for up to one year now—because we had a very uneven playing field. The police told me in these consultations how difficult that was to navigate with different police forces.

I think Canadians need to understand that this has been done in Australia, where it's up to two years; in the United Kingdom, where it's up to one year; in France, where it's up to one year; in Belgium, where it's up to one year; and in Sweden, where it's up to 10 months. There's no specifically correct number, but I think the complex investigations contemplated by modern policing are going to require that the data be held for a reasonable amount of time. I don't know if it's one year or 10 months, but it is a certain length of time.

Rhonda Kirkland: Thank you. That answers my question.

The Chair: Thank you.

I'm sorry, Ms. Kirkland. Time is up.

Rhonda Kirkland: See. This is exactly what I mean. I need more time with you.

The Chair: We always love to hear from you.

Now, we'll hear from MP Acan for another six minutes, please.

Sima Acan: I have no preamble. I promise. Time is essential.

Thank you very much for coming today, Deputy Chief Nick Milinovich. It's good to see you here.

My question is going to start with an earlier comment by MP Baber. He said law enforcement already has the ability to seek a search warrant and ask Google to comply with requests for information, and he asked whether that was correct.

Could you please explain the issues that law enforcement is currently facing?

D/Chief Nick Milinovich: I'm happy to have some of that conversation, but we would have to be here much longer than six minutes in order for me to do that.

The reality is that if we look at the legislation surrounding lawful access, the last time there was a substantial update was prior to the development of Google. If you imagine us operating right now, very simply put, we are delayed in our ability to secure information. We are not as effective as we could be, and we are certainly not as effective as some of the other Five Eyes countries are. We are hamstrung by outdated legislation, and it needs to evolve.

It is virtually the foundation of every complex investigation we complete. Normally, it begins with a production order and may result in a number of other different judicial authorizations, but we're receiving them slower than we should and not with the level of detail that we should have in order to accomplish the roles we've been provided. It's a difficult spot to be in.

I'll give you an example. If we were to watch an extortion happen in Peel, and the investigators go out, do their investigation and identify a corner store that captured that extortion on video, with the person speaking on a cellular telephone, we may write a production order for that tower site. The results of that production order, in some jurisdictions, could take up to 30, 45 or 50 days. In that time, we've lost evidence. We've lost the opportunity to prevent additional crimes. It doesn't happen all the time, but that's one of the big issues that we are dealing with.

There's an opportunity to be more effective and more efficient in our investigations through enhancements to the legislation surrounding lawful access.

● (1935)

Sima Acan: I learned that Canadian governments have been trying to pass lawful access legislation since the late 1990s. It's been more than 25 years. It's a long time. It means that lawful access has been studied here for hours and hours over the last 25 years. Bill C-22 has also undergone hours of consultations, and it is supported by a charter statement outlining how it impacts charter rights, especially those in section 8.

From a policing perspective, would you say Bill C-22 does not interfere with section 8? Do tools such as the confirmation of service demand respect those rights?

D/Chief Nick Milinovich: It's difficult to comment on every single scenario, but from my perspective, as it sits, Bill C-22 is charter-compliant. If it wasn't, I wouldn't be here asking for its endorsement. Outside of the charter and judicial oversight and consideration, there are a variety of other avenues where its authenticity and congruence with privacy interests will be tested. I anticipate that's going to happen.

Going back to your original point, the early 1990s—before Google and before the iPhone was developed—was the last time we had any significant legislation. That is why I'm here on behalf of my organization, on bended knee, asking for help to protect our community.

Sima Acan: Deputy Chief, you have worked on lawful access in past legislation and have been in policing for a very long time. Would you say holding metadata for up to a year, as worded in the legislation—up to 12 months—is reasonable for complex investigations?

I'm aware that tech companies often delete subscriber data in a shorter time frame.

D/Chief Nick Milinovich: That's a great question.

I tend to agree with Mr. Rankin. There has to be a timeline. We need to require people to keep that metadata to a certain level, because it's not as though a crime happens and we immediately arrive at the opportunity to collect this stuff. Crimes, and particularly more serious ones, don't have a statute of limitations. We're not talking about theft from a grocery store. We're talking about child exploitation or transnational crime, and that information can become incredibly valuable to the investigative community and policing.

Of course, I understand people's concerns about it in terms of a private citizen who commits no crimes. I understand that, but the reality is that nobody is going to look at their metadata, because they aren't doing anything wrong from the policing perspective. When you're a criminal and you're targeting our communities, it's the longer the better for us.

Sima Acan: Can you simplify it? Could you highlight how this data can be used to quickly resolve a case related to extortion or, as you said, child sexual exploitation?

D/Chief Nick Milinovich: Imagine the parallel. Everybody's familiar with physical forensics. That's something that's well accepted. We've all seen *CSI*. I think most people understand it. You can leave a trail behind at a crime scene that can be collected by the police and held in perpetuity.

We've made a number of arrests decades after a crime has occurred because we've been able to collect that information and hold it. Digital evidence is very similar to that. It's a footprint. It is as important to contemporary policing and public safety as forensics is to us.

Sima Acan: I believe my time is over.

The Chair: You are correct.

Let me move to Madame DeBellefeuille for six minutes, please.

[*Translation*]

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

First, Mr. Rankin, I want to thank you for speaking French, because I don't know whether my anglophone colleagues would have tolerated that 80% of the testimony not be in their official language. It's very difficult to concentrate and understand everything when listening to interpretation. So thank you very much. It was a long statement, so I wanted to thank you.

My question is for you, Mr. Smith. The Canadian Chamber of Commerce noted that Bill C-22 raises concerns and creates unpredictability because it's unclear who will be covered, due to the lack of definitions, which will be specified by regulation.

You seem to share this concern. Do you think some sectors or suppliers should be excluded? I'll give you the examples of Interac or Desjardins, whose representatives told us they should be excluded. Do you think we should specify in advance which sectors are excluded from the definition of primary suppliers, while still leaving the government some regulatory leeway, even as we try to narrow the range of primary suppliers?

Do you think specifying primary suppliers or setting out exclusions, for example, could be a reasonable solution?

● (1940)

[*English*]

Eric Smith: Thank you for the question. I'll be speaking in English.

We represent the telecommunications industry. It's well understood that telecommunications providers will be considered core providers. We haven't really turned our attention to how other sectors would fall under that category versus electronic service providers. We know we will be covered, and that's really been the focus of our attention to this bill.

[*Translation*]

Claude DeBellefeuille: It will be covered in both parts. Do you agree with it being in part 1 and part 2 of the bill?

[*English*]

Eric Smith: We have concerns about the bill itself, but in terms of your question about who should be covered by the bill, we understand that we will be covered by part 1 and part 2.

[*Translation*]

Claude DeBellefeuille: Mr. Rankin, you've led the consultations. If I recall correctly, you told us from the outset that you had the privilege, I think it's fair to say, of being the first chair of the National Security and Intelligence Review Agency.

Personally, I think the agency is a great idea. It's great to have it, and I believe in the work it does. The government has decided to make drastic cuts to the agency. It has clipped its wings by reducing its ability to investigate and lead more extensive investigations. The agency's budget was cut by 15%, or $2.5 million out of a $17 million budget. That's a pretty significant cut.

You chose not to invite Justice Deschamps, the current chair of the agency, to the round table. She told us she hadn't been invited to appear. I must tell you that this came as quite a surprise.

When she appeared before the committee, she recommended that amendments be made to the bill. At the Bloc Québécois, we will be presenting and supporting these amendments. I think the government is well aware of our position on this issue. Justice Deschamps told us that it would be important for her and for the agency, and especially to reassure Canadians, that the agency be notified in real time, as is the case for the intelligence commissioner. This would allow the agency to document decisions rather than having to rely on a retrospective investigation. We estimate that the agency would be informed about a year and a half after the interventions. I find these amendments very reasonable, especially since they wouldn't cause any delays, because she doesn't have access to the decisions.

During his appearance, the minister told us that granting this authority would slow down the process. The intelligence commissioner, former Justice Noël, told us that he did not share that view, that there would be no delays and that, in his view, it was entirely normal for her to be notified in real time.

What is your opinion on the matter, Mr. Rankin?

Hon. Murray Rankin: First, I'd like to thank you for your comments about my French. I really appreciate that, but if I may, I'll answer your question in English. I spent many years in British Columbia, and my French is a bit rusty.

[*English*]

I'm going to try to answer your excellent question in English.

Madam Justice Deschamps is somebody who succeeded me and is doing an excellent job at NSIRA. I am aware of the budget cuts, and I share your deep concern about them.

On the issue of the role for NSIRA, however, I point out that it is a body that does after-the-fact reviews. It has no current mandate, as contemplated in Bill C-22, for an oversight role. However, the intelligence commissioner has that role of reviewing ministerial orders. The commissioner already has an oversight role.

I don't think NSIRA, in my judgment, is set up for that kind of role. What I do think would be helpful is if NSICOP and NSIRA were asked to review later—not on a case-by-case basis, as I think you're contemplating, but overall—how the system is working. I think that would be very valuable.

● (1945)

[*Translation*]

Claude DeBellefeuille: I understand your—

The Chair: Mrs. Bellefeuille, unfortunately your time is up.

Mr. Caputo, you now have the floor for five minutes.

[*English*]

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

I want to thank all of the witnesses.

Deputy Chief Milinovich, I took heed of what you said. My colleague Ms. Acan asked you a question and you said that it was going to take a lot longer than six minutes, and I understand why. This isn't easy stuff.

This is complex stuff: how metadata leads to an offender, how a production order is authorized.... I mean, we haven't even gotten into that. I don't think that even once we've talked about the test for getting a production order. I think Mr. Van Laer did very briefly last time, but we haven't even talked about that here. That's part of the point I've been making. I know that my Liberal colleagues may think I'm a broken record, but the reality is that this is not easy stuff. This is where we have had lawyers come in here and disagree: knowledgeable lawyers, people who have practised law for a great deal of time.

I would love to hear more from you. I know that extortion is a huge issue in your area. You and I spoke—I believe it was just last month—and I really appreciate your passion for trying to bring safe streets to the Peel region. I echo that.

The thing that stands out for me—and this goes for all of our witnesses here—is that we all want safe streets. We all want to put bad people in jail. We all want people who hurt kids to go to jail and—I can say on this end—for a very long time. I would hope that my Liberal colleagues would join that, yet here we are, on the precipice of having to deal with a bill that has huge ramifications and huge implications.

I'm going to ask you just one brief question, Mr. Rankin. Was there one recommendation that you really hoped would have made it in here and didn't?

Hon. Murray Rankin: First of all, thank you very much for the question, MP Caputo.

I can't think of.... No, I can't answer that in such a simple way. I can't.

Frank Caputo: Fair enough.

Here is the reality, Mr. Chair. My friend and colleague Mr. Powlowski, when he was asking questions, talked about how he was still figuring this out. We are all still figuring this out. That's why I referenced Deputy Chief Milinovich's comment on how much time we have.

One theme that I've been stating throughout, and that I've been stating publicly and privately, is that we need more time with this bill. Yes, we've had three meetings. That's not nearly enough. These have been exhausting meetings. They've been going on for four hours. We're into the fourth hour, and we don't know basic things, such as how long metadata should be retained. I don't think we've actually gotten into the technical nature of how metadata leads to an arrest, which leads to a charge, which leads to a conviction. We haven't even touched on that. We have not touched on what the U.K. does, what Australia does, what the EU does or what Sweden does. We've heard it's 10 months, one year or two years. We have not gotten into that.

Speaking as somebody who wants to see bad people put behind bars, I know that we have to balance it with getting it right, period. I don't think anybody around this table wants to have legislation that will not stand up constitutionally. For that reason, I will be moving a motion. The clerk has received copies in both English and French, I believe.

This should not come as a surprise to any of my colleagues. I think we as Conservatives have been very transparent on this. We have been transparent on the necessity for more meetings.

Mr. Chair, as it stands right now—as it stands right now—we are going to hear from witnesses on Thursday, yet amendments are due tomorrow. We will actually be hearing from officials when the deadline for amendments has passed.

I checked with Mr. Rankin. I think we should have an hour or two with just him. It's been a major failing of this meeting, alone, that we crammed in 12 excellent witnesses who could probably have had an hour on their own—each one. We crammed them in, sometimes getting only two rounds.

With that in mind, I am putting forward this motion:

> That, in relation to the ongoing study of Bill C-22, an Act respecting lawful access,
>
> a) the study be extended to accommodate further examination of Part 2 of the bill which would enact the Supporting Authorized Access to Information Act, provided that the following witnesses appear separately, for at least one hour each:
>
> 1. the Minister of Industry, in relation to the impact on electronic service providers and their industry,
>
> 2. the Minister responsible for Canada-US Trade, in relation to trade and security implications raised by American lawmakers,
>
> 3. the Secretary of State (Combatting Crime);
>
> b) the committee receive an additional 8 hours of witness testimony, provided that the committee prioritize another briefing with departmental officials and hearing the testimony of representatives from Signal, NordVPN, OpenMedia, Centre for Free Expression, Canadian Constitution Foundation, Canadian Muslim Public Affairs Council, Migrant Workers Alliance for Change, and the testimony of Glenn Greenwald, Safiyya Ahmad, Noura Aljizawi, Teresa Scassa, and Jane Bailey, in addition to additional testimony deemed relevant by the committee;
>
> c) the chair be authorized to seek additional meeting time to accommodate this testimony in a timely manner;
>
> d) the deadline for submitting amendments be extended until the testimony outlined in this motion has been received;
>
> e) the chair only be authorized to schedule a meeting for the purposes of clause-by-clause consideration of the bill after the witnesses listed in part a) have appeared, and the number of hours of testimony in part b) have been received.

Mr. Chair, we owe it to the people who have appeared and who have told us of the necessity for this bill, we owe it to the victims and we owe it to Canadians to get this right and to get this right the first time. That is why I'm moving this motion.

I implore my colleagues to accept this motion. Let's get this bill done. Let's explore it, and let's get it done right.

Thank you.

● (1950)

[*Translation*]

The Chair: Thank you, Mr. Caputo.

Witnesses, this concludes your appearance. We won't keep you any longer. Given that the motion has been moved, we'll certainly spend the next few minutes discussing it. Therefore, we won't deprive you of the pleasure of returning home or wherever you'd like to go.

[*English*]

I'm happy to say that your day is over. Ours is not yet over, because we'll have to discuss that motion. We are obviously very grateful for your participation, either virtually or in person. Your views have been quite clearly heard, but not completely so. We look forward to more possible engagement with you in the future.

Have a great night. We won't suspend and shake hands, but you understand why we'll now focus on our own internal work. Thank you.

[*Translation*]

Ms. Kirkland, the floor is yours.

[*English*]

Rhonda Kirkland: Chair, I'm really concerned that we are just not spending the time necessary to get this right. When I first spoke to departmental officials, before we even started studying this bill here in committee, I assured them that we want, for those who are committing the most heinous crimes, the best possible lawful access regime that could potentially do the job that it's supposed to do, but what we don't want is to have one thing at the sacrifice of another.

As an example, we had today, in our committee time, four hours. One hour only had two rounds. There were issues of privilege, and these were brought up simply because we don't have time. We're not getting the information that we need in a timely manner, and that's not anyone's fault. It's the clock's fault.

The only fault that we can place on this is the fact that the government, to be fair, has decided that it wants to ram this legislation through and race to royal assent, as I have said several times. This is not doing the justice that this type of legislation deserves. Canadians deserve to hear everything. I said before that I could ask these witnesses the questions that I have privately, but that is not appropriate for all Canadians. They want to know the answers to these questions.

I'm specifically shocked and annoyed by words that were used by the mayor of Brampton. Although I respect him greatly, it's not dithering to properly look at legislation and take it apart piece by piece. That is our job. If we're not going to do our job, then what are we here for? Is it the job of the opposition, as well, to just sit back and say, “Yes, yes, yes”, and be yes-people?

It's just outrageous to me that we've spent such little time. Asking for eight more hours seems very congenial. It should be easy to do. If we do four-hour meetings again, that's two more four-hour meetings.

I know we're tired, but this is our job. If we don't get this right, then we could be causing lots of problems going forward, and I fear that we already are. We've seen news reports. Anyone who has reached out to my office has said, “Yes, we understand the need for lawful access, but my concerns are regarding my privacy and my safety.”

I implore everyone on this committee to take this motion seriously. It is made in good faith. I want to do my job, and I want to do my job effectively. I hope that everyone on this committee wants to do their job effectively to properly scrutinize this bill and to get it right. That's truly all we're asking for.

With that, I will leave it. The only possible thing I would like to mention is the idea of amendments being due before we finish hearing testimony. I don't understand that at all, and I don't think it's just because I'm a one-year, new parliamentarian.

● (1955)

The Chair: You may have been here for only one year, but you sound very experienced.

Let me turn to MP Ramsay.

Jacques Ramsay: I appreciate the views of Mr. Caputo and Mrs. Kirkland. I think we have a solution that will appease everyone, so we move to adjourn debate.

Rhonda Kirkland: How is that a solution?

Frank Caputo: How's that a solution?

[*Translation*]

The Chair: This is a dilatory motion that we must vote on immediately to adjourn the debate. To be clear, this isn't about adjourning the meeting, but adjourning the debate.

Who is in favour of this motion to adjourn the debate?

I think it's quite clear that the motion is—

[*English*]

Frank Caputo: We oppose. It should be on the record so that we—

The Chair: Okay. Do you want it on the record as on division?

Frank Caputo: No, it should be on the record. I think we should—

The Chair: Okay, if you want a roll call vote, we can do that.

(Motion agreed to: yeas 6; nays 5)

● (2000)

[*Translation*]

The Chair: Mr. Ramsay, the floor is yours.

Jacques Ramsay: I'd like to introduce a new motion:

> That the committee extends its study of C-22 by inviting witnesses to appear on Thursday, May 28 from 4:30-6:30 p.m.;
>
> That the amendment deadline be extended to Monday, June 1 at 5:30 p.m.;
>
> That the first hour of the meeting of Tuesday, June 2 be on Bill C-221, and receive testimony of the sponsor of the bill—

Claude DeBellefeuille: Sorry to interrupt you, Mr. Ramsay.

Mr. Chair, can we get a copy of the motion so we can read it?

The Chair: We will listen to Mr. Ramsay, then ensure everyone has a copy of the text.

Mr. Ramsay, the floor is yours.

Jacques Ramsay: I'll continue:

> That the first hour of the meeting of Tuesday, June 2 be on Bill C-221, and receive testimony of the sponsor of the bill, Mel Arnold;
>
> That the second hour of the meeting of Tuesday, June 2 consists of relevant department officials on the topics of main estimates, and on Bill C-22;
>
> And that clause-by-clause consideration of C-22 begin on Thursday, June 4th.

The Chair: Mr. Ramsay, do you have an English version? Can you read it in English? That way, it can be interpreted into French.

Jacques Ramsay: Yes.

[*English*]

Wait just a moment.

[*Translation*]

Claude DeBellefeuille: Mr. Chair, why don't we have a copy of the motion?

The Chair: We'll find out what's going on.

[*English*]

Jacques Ramsay: All right, in English it reads:

> That the committee extend its study of Bill C-22 by inviting witnesses to appear on Thursday, May 28, from 4:30 to 6:30 p.m.; that the amendment deadline be extended to Monday, June 1, at 5:30 p.m.; that the first hour of the meeting of Tuesday, June 2, be on Bill C-221 and receive testimony of the sponsor of the bill, Mel Arnold; that the second hour of the meeting of Tuesday, June 2, consist of relevant department officials on the topics of the main estimates and Bill C-22; and that clause-by-clause consideration of Bill C-22 begin on Thursday, June 4.

[*Translation*]

The Chair: Thank you.

We'll need this information to be sent to us by email, that is, in writing. The clerk will help with that. Please keep an eye on your devices. The motion will be sent in both French and English.

While the information is being sent, Mr. Caputo, would you like to speak? You're on my list.

[*English*]

Frank Caputo: I would respectfully ask that we suspend, and then I'll create my intervention once I've seen the motion in writing. I would like to actually see it in writing, please.

[*Translation*]

The Chair: We're going to suspend the meeting, but I want to make it clear that at 8:15 p.m., we'll have to conclude the debate because we don't have enough resources to go past 8:15 p.m.

● (2000)

_____(Pause)_____

● (2005)

The Chair: We're resuming the meeting.

Thank you for your patience. I think everyone received the motion proposed by Mr. Ramsay, in French and English.

Mr. Caputo, the floor is yours.

● (2010)

[*English*]

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

I thank Mr. Ramsay for the motion, although I think our motion is far superior.

Somebody is going to have to explain some logic to me here. Maybe I missed the boat. When I first raised the issue about officials, I did that in what I believe was good faith. It came about through a private conversation where I said that there are some issues here.

We heard from officials for one hour on this bill. When we heard from officials in the one hour, we had very few answers to the technical aspects of the bill. I will reiterate: What we have heard so far on this bill doesn't relate to the technical aspects. It relates to the philosophical aspects. Ninety per cent of what we've heard relates to the philosophical aspects. Even when we hear from police officials, they say that they really need this because it will help them track down people who do bad things. Well, okay, but we haven't really gotten into the mechanics of it, if we're being honest. We haven't gotten into the mechanics of it as far as how that happens.

I challenged Professor Geist on this. I don't know if anybody remembers. He was here and I asked him about metadata. I asked him what he thought. He said that a year is far too long. He said, “30 days”. I asked him what he'd say to the fact that there might not even be an investigator after 30 days. Mr. Van Laer talked about that. Sometimes you have to get a production order. Sometimes you don't know these things. He said that whatever you do, it has to be evidence-based. That was his response.

Can we say that so far we have figured out what that number should be? We've heard about stuff that's happening elsewhere in the world—in Sweden, it's apparently 10 months, and in Australia, it's apparently two years—and things like that. That is the very reason I think the officials are so vital. We have not gotten into the technical aspects of this, so when we are talking about this, I still think we need to hear from officials a whole lot more.

I'm just going to look at this motion here. The amendment deadline goes to 5:30 on Monday. Yes, we hear from witnesses on Thursday the 28th, but we run into the exact same problem: We have amendments due on Monday, we have officials on Tuesday and then we go to clause-by-clause on Thursday. Why are we hearing from officials after amendments are due?

I'm saying this rhetorically. I'm not expecting an answer. I think I would get no answer anyway.

Mr. Powlowski looks like he's chomping at the bit to give me an answer. He's just mastered this bill in the last 45 minutes or something like that.

I don't mean to make light of this. I take him at his word when he says, “We don't really get this.”

Okay, Ms. Acan really gets the bill.

Sima Acan: He didn't say “we.”

I get it, yes.

Frank Caputo: I am still processing what is in this bill. As a result, in order to fulfill our obligation as His Majesty's loyal opposition, we should have the right to hear from officials fulsomely before we have to submit amendments. Otherwise, we are essentially going to a glorified clause-by-clause because, in that case, we're going to hear from officials after amendments are in, which we would normally do in a clause-by-clause setting anyway. We're almost postponing the unavoidable. We're not really following a proper process in that.

I reiterate that there has been substantial questioning on this bill, and dare I say, from some people, substantial opposition. We heard today that a lot of people are really in favour of this bill. We have a group that is quite in favour of the bill. We have a group that is quite opposed to the bill. Our job is to try to find some middle ground that puts bad people behind bars and ensures that privacy and charter rights are protected. I think everybody around this table would want to see that. How do we do that when we have amendments that are due before we hear from officials? To me, it is eminently reasonable that we would hear from officials before amendments. I don't understand why we wouldn't do it.

For instance, let's look at part 1, “reasonable grounds to suspect” versus “reasonable grounds to believe”. We heard about the lower threshold from Commissioner Carrique. The only time we actually talked about reasonable grounds to suspect versus reasonable grounds to believe was when I asked the question.

My recollection of reasonable grounds to believe is that a peace officer personally or subjectively believes that an offence has been committed—not suspects—and that the belief is objectively reasonable. That is reasonable grounds to believe, or it was five years ago when I was still practising law.

● (2015)

Anthony Housefather: I have a point of information, Mr. Chair.

The Chair: A point of information is not really a point of order, but....

Anthony Housefather: I want to know when we have to cut off resources for the meeting—

The Chair: That's a good question.

Anthony Housefather: —because if we continue this, we will have amendments due tomorrow and clause-by-clause starting on Tuesday. I want to understand what time we would stop this.

The Chair: That's a point of order, which is disguised as a point of information.

I'm not a lawyer, so you would be better than me at describing it, but that's a very fair statement because I was going to make that statement.

We have three minutes before we need to adjourn this meeting.

As MP Housefather has said, if we don't vote on that motion, we have the existing motion, which prevails. That means we're going into clause-by-clause work next Tuesday, June 2, and the deadline for amendments is tomorrow. I'll let you know that because we have a default motion, default agenda, which we have voted on. We have an opportunity now to vote on a different agenda. We need to do this in the next two minutes, now.

Are we ready to vote on that?

Frank Caputo: I still have the floor, Chair—

The Chair: Yes, Mr. Caputo.

Frank Caputo: —unless Ms. Kirkland really wants the floor.

Rhonda Kirkland: I do.

The Chair: You have two minutes, Ms. Kirkland.

Rhonda Kirkland: I have a question. What's Thursday? What would we do in the next meeting?

The Chair: Thursday, we have the minister for one hour on main estimates, and we have two hours of.... We have one hour for the minister and one hour for officials, and then we extend for one more hour with the officials on Bill C-22. The three hours on Thursday will be one with the minister, one with officials on main estimates and the last one on Bill C-22.

Rhonda Kirkland: Yes, I want to ask a question, but I also don't want to cede the floor to ask the question. That's what I'm concerned about.

I don't understand at all how this is a solution. I know that Mr. Ramsay said, “Oh, I have a solution: Let's adjourn debate on your motion and let me introduce this beautiful motion, which is the solution to all of our concerns.”

The solution seems to be to leave in place the same scenario, where amendments are due before we have heard from department officials again, and to add an extra two hours for witnesses. Quite frankly, we had 18 witnesses here today. I know that Mr. Caputo said we had 12. We had 18 witnesses here today: 18 people and maybe 12 or 13 organizations. We didn't get to ask them questions.

My concern with this is that we had no time. We don't have any time. This government is just frankly abusing its power, in my opinion, by ramming through legislation without giving the opposition a chance to properly question witnesses so that we can pass a bill that is done right. We want a bill that is done right. We want it.

I'm a little bit blown away. In fact, I'm a lot blown away that we don't want to do our jobs, that we want to limit the amount of time that we're studying this bill and that we just want to go, go, go, to the detriment of Canadians and their privacy and their rights. Quite frankly, I'm baffled that everyone at this table is okay with that. I really am. I don't really understand it at all.

When I first started hearing about this bill and looking at it—

● (2020)

The Chair: I will have to interrupt you very soon.

Rhonda Kirkland: Okay. I will end with this, then.

Are you interrupting to end the meeting? Is that what you're saying?

The Chair: Yes, because we don't have any resources anymore, meaning that the interpreters and the technical people need to go.

Rhonda Kirkland: Yes, I—

The Chair: Let me also add another point of information. I can suspend, but it means that we don't have the minister on Thursday. The minister is supposed to come for the main estimates on Thursday. If I suspend the discussion, which is possible, then we lose the minister on Thursday.

I normally adjourn the meeting, which I will do in a second. That means we are going to follow the existing motion setting the agenda, unless there are conversations outside of this meeting in the next hours to adjust it accordingly.

Let me therefore adjourn the meeting and wish everyone a good night.