HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

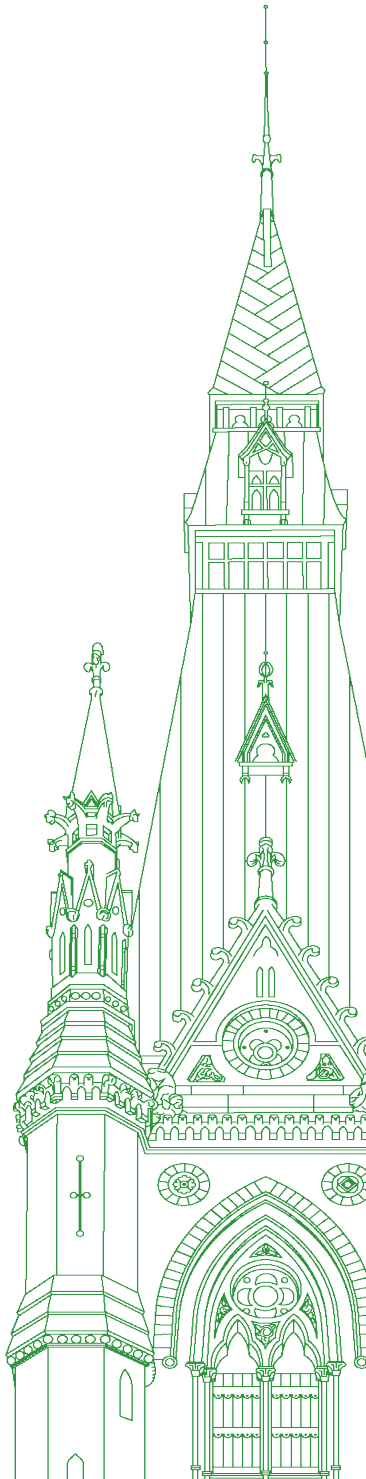
45th PARLIAMENT, 1st SESSION

Standing Committee on Public Safety and National Security

EVIDENCE

NUMBER 036

Tuesday, May 5, 2026



Chair: Jean-Yves Duclos

Standing Committee on Public Safety and National Security

Tuesday, May 5, 2026

● (1555)

[*Translation*]

The Chair (Hon. Jean-Yves Duclos (Québec Centre, Lib.)): I call this meeting to order.

I want to thank everyone for joining us.

First of all, I apologize for all the emotions you may have gone through over the past few hours. I'm thinking in particular of the clerk. There were changes in schedules, votes, assigned seats, unassigned seats, reassigned seats and so on. I thank you all for your kindness and indulgence.

Welcome to meeting number 36 of the Standing Committee on Public Safety and National Security.

We're meeting today as part of our study on Bill C-22, an act respecting lawful access.

First, I'd like to welcome the witnesses, who are all senior officials. The ministers will be joining us in about an hour.

We have with us, from the Canadian Security Intelligence Service, Ramzi Nashef, director general; from the Department of Justice, Kimberley Gibner, Normand Wong and Anne-Marie LeBel; from the Department of Public Safety and Emergency Preparedness, Shannon Hiegel, Mike McGuire and Fenton Ho; and from the Royal Canadian Mounted Police, Richard Burchill.

Mr. McGuire, we'll start with you, please. You have the floor for five minutes.

[*English*]

Mike McGuire (Director General, International and Border Policy, Department of Public Safety and Emergency Preparedness): Thank you, Mr. Chair and honourable members of the committee, for having us here today.

My name is Mike McGuire. I'm the director general of international and border policy at Public Safety Canada. I'm pleased to be here with colleagues, as was just mentioned, from the Department of Justice, the Department of Public Safety, the RCMP and CSIS to answer technical questions on Bill C-22, an act respecting lawful access.

Lawful access is a familiar issue that has been studied by Parliament in the past, most recently by the National Security and Intelligence Committee of Parliamentarians, which issued a special report last year calling for lawful access legislative reform.

[*Translation*]

Bill C-22 seeks to address fundamental and well-documented gaps in Canada's lawful access framework. The online environment has facilitated, if not fostered, the communication, coordination and concealment of criminal activities and those of threat actors. The widespread use of mobile devices, Internet-based communications, messaging platforms and other emerging technologies has fundamentally transformed how crimes and threats to national security are planned, executed and investigated.

At the same time, Canadian police services and CSIS face increasing challenges in obtaining information critical to investigations in a timely manner. Bill C-22 seeks to address these challenges while maintaining strong safeguards, including respect for the Canadian Charter of Rights and Freedoms and the protection of Canadians' privacy.

[*English*]

The provisions in Bill C-22 are grouped under two key themes. First, part 1 of the bill modernizes Canada's legal authorities to support police and CSIS in obtaining timely and lawful access to digital information needed for investigations, with each tool carefully designed to take into account the type of information that will be collected and the privacy interest it engages.

This includes the creation of a new confirmation of service demand, which would allow police to confirm whether a telecommunications service provider offers or has offered service in relation to a specific identifier, for example a specific telephone number or IP address. The scope of this tool has been deliberately limited to a yes-or-no confirmation, and it pertains only to telecommunications service providers.

Part 1 would also create a new production order from narrowly defined subscriber information, such as name, address and basic information about the services provided, and update existing search warrant powers to better reflect computer searches.

In addition, it would establish new authorities to facilitate lawful requests from Canadian law enforcement to foreign electronic service providers and enhance international co-operation in criminal matters involving electronic data.

These measures are intended to ensure that where lawfully authorized, investigators are able to act in a timely and effective manner, bearing in mind that delays can result in serious and ongoing harm to victims in particular cases and circumstances.

● (1600)

[*Translation*]

Part 2 of the bill establishes a clear and modern legislative framework to ensure electronic service providers have the technical capacity to effectively respond to lawful access requests, meaning access already approved under existing legislation, such as the Criminal Code or the Canadian Security Intelligence Service Act.

Canada is the only western democracy without a comprehensive legal framework requiring electronic service providers to develop and maintain such technical capabilities. With the exception of an antiquated licensing regime dating back to the 1990s, collaboration in this area remains largely voluntary and uneven.

Part 2 of Bill C-22 sets for core providers minimum technical capability requirements aligned with international standards and provides the Minister of Public Safety with the authority to issue targeted and flexible ministerial orders when specific capabilities are required to meet operational needs.

[*English*]

Safeguards related to this new framework are embedded in the bill. For example, ministerial orders would be subject to approval by the intelligence commissioner and would be proactively reported to NSIRA. Privacy and cybersecurity considerations are explicitly included in the legislation. Data retention obligations are restricted, and public annual reporting is required.

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.

Finally, part 2 establishes tools to promote compliance, including inspections and administrative monetary penalties.

[*Translation*]

Together, these mechanisms aim to ensure Canadian law enforcement and intelligence agencies have the tools they need to do their important work while maintaining strong accountability and transparency.

Mr. Chair and members of the committee, my colleagues and I would be happy to answer your questions.

The Chair: Thank you, Mr. McGuire.

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

[*English*]

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

Thank you to all of our witnesses. It's so great to have so many people here around the table for such a complex issue. We're going to get to know each other very well in the coming two parliamentary weeks.

I never know who to direct my questions to, because there is a lot of expertise here. Whoever is best to answer this, please let me know.

I've looked at the definitions. I've looked at the definitions of "systemic vulnerability", at how it incorporates the definition of encrypted data to some degree, and at the provision, in part 2, that says a service provider does not have to do anything that would create a systemic vulnerability. I'm going to ask a very direct question. Will this bill cover encrypted data? Secondly, is it intended to be that way? I assume that would be yes. Will this bill cover encrypted data? Could somebody please help me with that?

Shannon Hiegel (Director General, National Security Policy Directorate, Department of Public Safety and Emergency Preparedness): Thank you very much for the question. I'm Shannon Hiegel, director general of national security policy at Public Safety Canada.

The bill is in fact encryption-neutral. We want to make sure that, where encryption is used.... There are different ways encryption can be used and different ways in which companies employ it. Therefore, we don't want to leave out the possibility for those companies that may employ encryption where there are keys available and it can be decrypted in a simple fashion.

Frank Caputo: Okay, but with all due respect, Ms. Hiegel, you say "where keys are available". This bill, as I read it, would require a key to be available, would it not?

Shannon Hiegel: Some companies already employ a type of encryption where they have the key. We're not asking for keys to be made if a company already has one.

● (1605)

Frank Caputo: Perhaps we're on different planes here, because my understanding of part 2, in reading it, particularly in proposed section 5, is that it talks about a base level that providers need to come up to. Am I making sense so far?

Shannon Hiegel: Yes.

Frank Caputo: If providers need to come up to that base level and they're not there yet, how do they not then have to create a key to come up to the base level that proposed section 5 says they have to come up to? Does that make sense?

Shannon Hiegel: Are you talking about somebody coming up to a level where they don't even have encryption? That's what I'm hearing you say.

Frank Caputo: No, I meant where there is a service of encryption provided. My question was, will that provider of encryption...?

Company A provides an end-to-end encryption service in messages. Will this bill require company A to create some sort of mechanism by which that data can be intercepted and by which the government or the state—when I say "state", I think you know what I mean, law enforcement—can access that encrypted data?

Is that clear?

Shannon Hiegel: Absolutely.

If a company has end-to-end encryption as part of its business service and its model, we are not forcing the company to decrypt that communication.

Frank Caputo: Okay. That's unclear at this point. When I read the bill, I thought, "Okay, that's it", but we've also seen correspondence here. If the target of this bill is not encrypted data, my suggestion is that we say flat out, "For greater clarity, this part does not apply to encrypted data", and then have a definition.

Does it make sense to do something like that?

Shannon Hiegel: I think we want to be a bit flexible when we talk about encryption. I apologize if the front part of my answer wasn't clear, but there are different types of encryption. If we talk about encryption without any qualifiers, that means that when companies do have keys and could decrypt for the purposes of an investigation where there's a warrant and a production order being provided, they could in fact still use those keys for that purpose.

Frank Caputo: What I'm talking about is a company whose "secret sauce", if you'll forgive my vernacular, is providing an encryption service. That is what it does. Company A provides a service that says terminal one to terminal two or contact one to contact two will be encrypted. That is its business model.

What I'm asking is this: Will Bill C-22 require it to be able to plug into that encryption and decrypt it for law enforcement?

Shannon Hiegel: No. If there are no keys and there's no way to decrypt it, and that's its business model, then the expectation is that this would be a systemic vulnerability for the entirety of its system, and there would have to be some discussion with government. The end of it is that we would not force it to put into its system a systemic vulnerability.

Frank Caputo: That is exactly what I was looking for, but based on my reading of the bill, when I went through the one definition and then into systemic vulnerability, that wasn't clear to me. My exhortation is this: As officials, please turn your minds to this, because I think there should be, one, an encrypted data definition and, two, something that very clearly says what you just said—that a decryption of encrypted data is a systemic vulnerability—or put it right in the definition of systemic vulnerability.

I know this is technical. I hope I'm being clear here.

The Chair: That may be very clear, but unfortunately we won't know what Ms. Hiegel thinks, because we need to turn to Madame Acan for six minutes, please.

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

Mr. McGuire and Ms. Hiegel, my questions will be on the technical side, so I believe you will be answering.

As we examine the evolving landscape of public safety and national security, it's essential to clearly understand the role of metadata. Metadata is often described as data about data that does not capture the content of communications but rather provides contextual information such as time, location, duration, origin or destination of digital interactions.

While it differs from content data, metadata can, in specific circumstances, support analytical insights and help identify patterns that are relevant to operational needs. This makes metadata a valuable operational tool for law enforcement and intelligence agencies, and it plays a critical role in enabling threat detection, risk assessment and investigative efficiency, particularly in an era when digital activity is deeply embedded in our daily lives.

Please correct me if I was wrong about or missed anything regarding metadata, but given this context, could you please clarify the scope of the information that law enforcement would be authorized to access under the legislation, and specifically confirm how metadata is distinguished from the content of communications in practice?

● (1610)

Shannon Hiegel: I'll start off and, if you don't mind, I'll turn it over to my colleague, Fenton. Then, if you'll give me a few minutes, I'll turn to the RCMP and maybe CSIS to explain how important metadata can be in their operations.

As you can see within the bill as it currently stands, we have not given a lot of specificity to what elements of metadata we plan on regulating. That's because we need to take the time to assess that with our investigative bodies and speak with industry about the ability to retain various types and for how long. We certainly do not assume.... Where we note that it's up to a period of one year, the expectation is not that all metadata points will be kept for up to one year. That's why there's a time period.

We've looked at international comparisons on this front, and we've come in about the middle. Australia holds its metadata for two years, and the U.K. holds it for about a year. There's always a bit of small print there, but generally that's what it is.

Through that process, we expect to narrow down what very specific types of metadata are the most important for investigations and then apply a timeline to that within the regulatory process. We will do our charter challenge at that point.

Fenton, is there anything you might like to add?

Fenton Ho (Director, Intelligence Policy, Department of Public Safety and Emergency Preparedness): Thank you.

I think the key idea here is that we're linking the metadata to capabilities that will support law enforcement. That's how we actually generate and derive what we need. The whole thing is that, as Shannon was saying, we'll be working very directly with law enforcement and with CSIS to determine what fields and how they support investigations, so that we can basically have a good, strong argument for why that is proportionate and why that's necessary to keep.

Ramzi Nashef (Director General, Canadian Security Intelligence Service): I have one quick operational point.

What we're talking about here is a better understanding of the pattern of communications, essentially. Through regulations, we'll work through the specific details of the types of metadata we'd be capturing. Generally speaking, from our perspective, the reason we would be doing that is to establish patterns of communication, in a warranted way, to be a building block for an investigation. Obviously, there are many other elements, but that's the sort of pattern we'd be looking for on our side.

Sima Acan: The next question could be probably answered again by you or by CSIS.

Bill C-22 introduces a new confirmation of service demand authority. This amendment to the CSIS Act is intended to allow authorities to continue obtaining necessary information in support of complex and advanced investigations.

How does this yes-or-no confirmation of service process introduced in Bill C-22 balance privacy considerations with investigative requirements? In what way does limiting disclosure to the existence of a service, rather than to subscriber identity, affect the nature and scope of information available to law enforcement?

Richard Burchill (Director General, Technical Investigation Services, Royal Canadian Mounted Police): The confirmation of service demand is very front-end, at the beginning of an investigation, to enable us to gather basic information to pursue an investigation. We have very little information—for instance, a phone number or an IP address. Just that yes-or-no confirmation from a telecommunications service provider gives us the ability to verify that this person is with this company. Then, we can start doing investigative work around that to get enough grounds to bring forward a production order to get subscriber information as a next step. We still have to build those investigative grounds in order to bring forward a production order to get subscriber information from a justice.

Although there are various ways that law enforcement and intelligence folks are able to get that information traditionally, that confirmation of service demand codifies that process and makes it disclosable. We have to document a confirmation of service demand. It goes on our file, is disclosed in court and can be questioned. We have reasonable grounds to suspect and to ask for the confirmation of service. Once it's obtained, then we still have to build investigative capacity around a production order to go to a justice or a judge.

● (1615)

The Chair: Thank you very much.

[*Translation*]

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

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

Ms. Hiegel, the minister told us consultations were held with certain groups between Bill C-2 and Bill C-22.

Can you confirm the current chair of the National Security and Intelligence Review Agency, Ms. Deschamps, was consulted on Bill C-22?

Mike McGuire: I can talk a little bit about the consultations.

Claude DeBellefeuille: I just need a yes-or-no answer. Do you know if Ms. Deschamps was consulted on Bill C-22?

Mike McGuire: Different types of consultations were held. The minister himself met with certain people, and there were also round tables.

Claude DeBellefeuille: To your knowledge, was Ms. Deschamps consulted? It's a pretty simple question, Mr. McGuire.

Mike McGuire: To my knowledge, she was not part of the round tables we organized.

Claude DeBellefeuille: This means the current chair of the National Security and Intelligence Review Agency wasn't consulted on Bill C-22, but a former chair was. That's what I understood from my readings.

Mike McGuire: For the round tables we organized, yes, but there were other consultations.

Claude DeBellefeuille: Don't you find it a bit odd that the current chair wasn't consulted on a lawful access bill?

When we see what's being done in the countries to which Canada compares itself, and that the agency's counterparts have an important role to play in lawful access legislation, don't you find that a bit odd?

Mike McGuire: We took a lot of information into consideration in our analysis. We also held various consultations and received various letters from stakeholders. Different methods were used to establish stakeholders' positions .

Claude DeBellefeuille: I'm just surprised, Mr. McGuire, because this is an important office. I'm surprised the agency's current chair wasn't consulted.

Did you consult the Privacy Commissioner?

Mike McGuire: Yes, absolutely.

Claude DeBellefeuille: You chose to consult the Privacy Commissioner, but not the current chair of the National Security and Intelligence Review Agency. That's my understanding.

Mike McGuire: We consulted the Privacy Commissioner.

Claude DeBellefeuille: However, you didn't consult the current chair of the agency.

I'm going to ask a question I've asked the Department of Justice team many times in the House. I'm not a lawyer, so I'd like to understand why you chose the lowest threshold for obtaining information.

I think reasonable grounds to "suspect" something seems like a very, very low threshold for obtaining information. Reasonable grounds to "believe" something would be a higher threshold. I don't understand why you chose this one.

Could you give us some examples of what reasonable grounds to suspect something might be? I have a hard time imagining what wouldn't be acceptable. I think any reason to suspect something can be reasonable. That part of the bill worries me. Could you give us tangible examples of what might be reasonable grounds to suspect something?

Anne-Marie LeBel (Counsel, Criminal Law Policy Section, Department of Justice): Thank you for that very good question.

Yes, we can give you some practical examples, and I may turn to my colleague from the RCMP to help out.

Before I do, I can explain why we chose that threshold. This is a legal threshold that already exists in the Criminal Code for other specific production orders, which target specific types of data whose privacy nature is less sensitive than others, including content obtained with a general production order.

Claude DeBellefeuille: Could you tell us what would be reasonable grounds to suspect something so I can clearly see the difference between this threshold and other thresholds and understand what your intention is?

Anne-Marie LeBel: Before my colleague gives you a tangible example, I'd like to add that reasonable grounds to suspect something is not just suspicion. There have to be observable facts. A police officer must have notes related to these facts when they decide they have reasonable grounds to suspect that an offence has been or will be committed.

In both of our tools, the condition is that there are reasonable grounds to suspect an offence has been or will be committed, but also that the information requested will be useful to the investigation.

● (1620)

Claude DeBellefeuille: Thank you, Ms. Lebel.

I would need that. I'm not a lawyer, and I'd like to get a better understanding, if I could.

I'd like to use the time I have left to understand something else. In part 1 of the bill, it says that "telecommunications service provider has the same meaning as in subsection 2(1) of the Telecommunications Act", whereas part 2 of the bill talks about an electronic service provider and a core provider. However, there is no definition in the schedule.

I want to understand why this very broad regulatory power is being given in definitions. People are wondering whether they'll be affected. Can you explain why there's no definition, why there's nothing in the schedule and why everything will be decided by regulation?

Anne-Marie LeBel: I think the question relates more to part 2, so the new act and schedule. I'll let my colleague answer it.

Shannon Hiegel: Yes, that's a question for me.

You're right to say that, in part 2, there's just a definition for an "electronic service provider".

It's a very broad definition, and that's important, because technology is evolving quickly.

The Chair: Unfortunately, I have to interrupt you, because the time's already up and I think it might be a long answer. We may come back to that later.

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

[*English*]

Dane Lloyd (Parkland, CPC): Thank you, Mr. Chair.

Thank you to the witnesses for being here today.

I'm going to start with Mr. McGuire.

Something I find contradictory in this bill—maybe you can explain how it's not contradictory—is that you're requiring electronic service providers and telecoms to create the systems to enable the interception of communications within their networks, yet later you say that nothing in this bill seeks to undermine the integrity of encryption networks. That seems very contradictory to me.

In light of the Salt Typhoon hack we saw in the United States.... It was later found that it was exactly the vulnerabilities created by the requirements under U.S. law to create these encryption back doors that allowed hackers to access this information.

Can you explain what this contradiction appears to be?

Mike McGuire: I'll start quickly and then turn it over to Ms. Hiegel.

The intent of part 2 is to ensure that electronic service providers have the technical capabilities to respond to lawful access requests that are authorized for law enforcement and for CSIS.

Shannon, do you want to add anything?

Shannon Hiegel: I'll start off and then I'll flip it over to Fenton.

We've taken a look at a multitude of other countries that have this type of legislation in place and have found ways to work with companies to pull the information out so that it can be provided to investigators for their specific investigations.

I don't feel that there's necessarily a contradiction between the two parts, because we are going to set objectives. We, the government, are not going to tell companies—or core providers, essentially—what and how they need to create—

Dane Lloyd: I understand what you're saying, which is that the government isn't dictating how the companies are to do it, but it is mandating the companies to do it, and in order to comply, companies may have to create vulnerabilities in their system that can be exploited by hackers. Wouldn't you agree?

Shannon Hiegel: I would say that companies create all sorts of changes within their systems for purposes that they see fit. Through this piece of legislation, we're hoping and we expect to find safe ways to maintain their cybersecurity, as Canada expects.

Canada, first and foremost, puts priority on cybersecurity—

Dane Lloyd: I'll interrupt you there.

If it comes to a choice between a company complying with the legislation and creating a vulnerability that can be exploited by hackers, what is the end goal or outcome of the Government of Canada?

Shannon Hiegel: I think the expectation is that, in consultation with government, we will find solutions to this. It is a problem that desperately needs a solution. Working with industry to be able to get information to the investigators to investigate so many crimes that are now going unsolved—

● (1625)

Dane Lloyd: If you can't find a solution, at least in the short term, is it acceptable to the government that telecommunications companies be forced to create systemic vulnerabilities in order to comply with the legislation?

Shannon Hiegel: There are partners we already work with right now, so I would question the idea that there's no way to be able to put solutions in place.

Dane Lloyd: The Canadian Chamber of Commerce has said that this legislation is going to force their members to create vulnerabilities in their systems. That's a pretty big stakeholder, including many stakeholders that the Government of Canada works with.

This is a big concern, so I just I want it clear: If the only way to comply with this legislation is to create systemic vulnerabilities, does the government still think companies need to comply with this legislation?

Fenton Ho: We're talking about various capabilities. It's not one universal capability. Also, these capabilities already exist right now. A lot of the major telecoms, because of the licensing regime, already have the capability to address certain requests from law enforcement or CSIS, so in that case, the bill basically creates a level playing field for what exists.

However, if you're looking at a particular application, a particular capability that doesn't exist, if it hits a systemic vulnerability, the answer would be no.

Dane Lloyd: I have 45 seconds left, so if I can get that in writing from you, please send that in writing.

In my last 45 seconds.... The Secretary of State for Combatting Crime said that many stakeholders are calling this an essential first step and that they need to broaden this legislation. Is the Department of Public Safety working on or envisioning a follow-up piece of legislation to expand the powers given under Bill C-22 at this time?

Shannon Hiegel: No, not at this time.

Dane Lloyd: Can you say that the department has done any studies on what the next steps would be, should this legislation pass, for follow-up legislation in this area?

Shannon Hiegel: No, we are very focused on the regulatory step that would follow, if we are successful in getting royal assent.

Dane Lloyd: Thank you.

The Chair: Thank you very much, MP Lloyd.

MP Powlowski, you have five minutes, please.

Marcus Powlowski (Thunder Bay—Rainy River, Lib.): I have a letter before me entitled “Joint Call for the Withdrawal of Bill C-22”, which is signed by a number of seemingly pretty reputable organizations, such as the British Columbia Civil Liberties Association, the Canadian Association of University Teachers, the Canadian Civil Liberties Association and the Canadian Council for Refugees. In it, they talk about the “enormous overreach of Bill C-22 and the unprecedented, open-ended powers it introduces”. Then it goes on.

There's one specific provision I want to ask you about, but let me read the whole paragraph. It says:

> Bill C-22 makes some improvements to Bill C-2's proposal for wide-ranging warrantless access to sensitive subscriber information. The warrantless demand power can now only be used to require telecommunications service providers to confirm if someone is a customer. However, Bill C-22's approach to subscriber data remains flawed, dropping the judicial authorization standard for a warrant from “reason to believe” to the far lower “reason to suspect” threshold despite Supreme Court decisions recognizing the significant privacy interests engaged by this form of data access.

If we're worried about overreach and if we're worried—as they are—about mass surveillance of all Canadians, I would tend to agree that “reason to suspect” seems a very low threshold for accessing potentially personal data. Does somebody want to answer this accusation?

Kimberly Gibner (Deputy Assistant Deputy Minister, Policy Sector, Department of Justice): I'll take that question.

I think my colleague touched on that and highlighted that there are all sorts of Criminal Code provisions that use the reasonable grounds to suspect standard. In this case, what you're looking at in terms of the subscriber information is essentially a name and an address. On the balance of that type of information with the privacy concerns, reasonable grounds to suspect was chosen as the appropriate standard.

Just to speak to your point about Spencer, what the decision said was that it was critical that there be lawful authorization, so since 2014, police have been calling for lawful authorization. That's what Bill C-22 does. It provides lawful authorization.

Marcus Powlowski: Now, for end-to-end encrypted services, like Signal, where the providers never possess the unencrypted data or decryption keys, these providers would not be expected to degrade their encryption to comply. Is that correct?

● (1630)

Shannon Hiegel: That is correct.

Marcus Powlowski: Okay.

Lastly, you talk about collecting metadata. What sort of metadata? If I'm on the Internet and if I'm sympathetic to the people of Gaza and searching about Gaza and inadvertently something comes up on Hamas, is there a reason for the government to further investigate me because of the possibility that I may be somehow doing things to promote a terrorist organization? What sort of metadata are you looking for? Metadata seems pretty broad. I mean, that's everything we do. If you put it into computer AI, you'd find something on Marcus Powlowski.

Shannon Hiegel: It's understandable to be concerned about that. What I would like to do is turn it over to my RCMP colleague, who, along with his team, is going to help define the very specific elements of metadata that are required. They will be regulated, but my colleague can give some specific examples.

Richard Burchill: I can give four examples of metadata retention that are helpful for law enforcement in an investigation. One is Internet transmission data, which includes time-stamps, IP addresses and device identifiers. As you can appreciate, we don't start an investigation immediately when something happens. When something happens and there's online activity, there generally needs to be a report made and an investigation generated. If we're looking to get metadata, there has to be a judicial authorization; there's criminality involved, and there are victims involved at the front end of this. By the time we get to the point where we're seeking the metadata, it's to try to link people to places. That's Internet transmission data.

Tower signalling data is also helpful to locate folks at a point in time when there is an offence that happened or a call, if it's a kidnapping or something, where we need to find the location of somebody who had a vehicle or a phone at a certain time.

The Chair: I'm sorry, but I have to interrupt you abruptly so we can move to Madame DeBellefeuille.

[*Translation*]

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

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

Ms. Hiegel, Bill C-22 still gives the intelligence commissioner an important role. Have you assessed the additional work the adoption of this bill could cause them?

Shannon Hiegel: Thank you for the question.

[*English*]

I apologize. I'm going to speak in English.

We actually have met with the intelligence commissioner himself and his staff to talk about the role. Once it is approved, he will be the second key. He has spoken to the fact that.... We have given some sense of what we expect and how many ministerial orders there may be on an annual basis.

[*Translation*]

Claude DeBellefeuille: [*Inaudible—Editor*] your assessment. How much do you think they'll be solicited with the adoption of Bill C-22? As you know, they tabled their annual report, which contains a record 14 decisions. Now, I wonder if there will be a lot of decisions. Did you assess the number of decisions the commissioner might have to issue?

[*English*]

Shannon Hiegel: His role is specific to the ministerial order approval process. He will be reviewing all of the information that was given to the minister when the minister made his or her decision on a ministerial order, which is a very specific request to put in place certain capabilities for a company that would not be included as a core provider.

[*Translation*]

Claude DeBellefeuille: That means it's exceptional. It's not going to be common. There aren't going to be a lot of decisions. The intelligence commissioner isn't going to be overwhelmed with decisions.

[*English*]

Shannon Hiegel: No, and he has confirmed that. We gave him some initial numbers around how many ministerial orders would come to him, and he was sufficiently satisfied that he could manage it.

[*Translation*]

Claude DeBellefeuille: Okay.

I know his office's budget wasn't increased to meet its obligations in Bill C-22, so I was wondering what the workload would be like.

You may not have time to answer this, but why didn't you include in part 2 a clear definition of “core provider”?

● (1635)

[*English*]

Shannon Hiegel: For a core provider, we do have a definition. What we expect to do is run through the regulatory process, where there will be classifications or classes—

[*Translation*]

Claude DeBellefeuille: There is none in the bill, Ms. Hiegel. It'll be dealt with in the regulation.

[*English*]

Shannon Hiegel: Yes, it will be in regulation.

[*Translation*]

The Chair: Unfortunately, I have to cut you off there. I apologize.

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

[*English*]

Frank Caputo: Thank you very much.

It's been helpful to have the officials. One thing I will say at the outset is that I feel like we need three hours with you. I don't say this in jest. This is a highly technical bill. We can't rush this. I have a list of about eight things I want to ask you about.

I'm looking up case law further to Madame DeBellefeuille's earlier point about the threshold of “reasonable grounds to suspect” versus “reasonable grounds to believe”. I haven't studied reasonable grounds to suspect in years. With regard to reasonable grounds to believe, I'm familiar with the Storrey decision that a person must subjectively believe that what they're doing is reasonable and that it must be objectively reasonable.

That probably means nothing to a lot of people, but these are difficult things to comprehend. When we're wrapping our heads around this, I think having you here for only one hour prior to clause-by-clause consideration is inadequate. I think we need you here a whole lot more, to be very candid. I'll leave that with you and with the chair and with my Liberal colleagues, because we have lots of questions, and I know I've just burned a minute here.

This is an important question that comes to the requirement for an electronic service provider to retain data for one year. Is that a de facto seizure that runs contrary to section 8? I understand that a search warrant is required, and that would be the search aspect. Normally there's the search and then the seizure. Is the compulsion to retain data a seizure in itself?

Shannon Hiegel: I'll attempt to just simply say that we have not equated the expectation of the retention by a company to a seizure within the context of an investigation, because there has been no production order or warrant approved by a judge. That would be my simple assessment of the scenario.

Do any of you have thoughts?

Richard Burchill: As you said, we need a judicial authorization in order to access that data. The timeliness of it is.... There are companies that already retain this metadata. There's not a consistent application of how that happens among telecommunication providers, which is what security and law enforcement would look for. When we're looking to access that data, the reason for the timeliness is that if they keep it for three days but you're one week into a kidnapping investigation, that data is gone, whether you are judicially authorized or not, whereas some companies will have it readily available.

Frank Caputo: I understand that. I'll tell you where I'm coming from on this. In this instance, the state or the government is compelling an action, and that action relates to information over which there is a reasonable expectation of privacy. That's why you need a warrant. The moment you say to provider A that they need to keep this, there's a reasonable expectation of privacy over what must be kept. Is everybody with me so far? Okay.

Does that not engage section 8? I might be out to lunch here, but I've been asked this question, so it's something I'm looking to explore.

Shannon Hiegel: Just as a point of clarity, when you say section 8, do you mean with regard to part 2 of the bill?

Frank Caputo: Yes.

Shannon Hiegel: Fenton, do you want to jump in?

Fenton Ho: Obviously, we've had discussions around charter statements and stuff about that. Part of the analysis on that point will be how we actually circumscribe our use of metadata. In this case, we are clearly not looking.... The maximum is one year. We're not saying it's blanket retention. In the process of developing the regulations, we would have to prove that they're necessarily in proportion with that amount of time. At that point, we can come to an understanding of what charter obligations arise from that.

Frank Caputo: Let's go along that line here. The one year is kind of the benchmark. Are you saying...? We could talk about this for the next 15 minutes—this is, again, very important—and I have 33 seconds. What you're saying is that one year is the maximum. It's not the minimum. It's not just the drop-dead date. It's only one year. Obviously, any date is arbitrary. Why is it a year? Why is it not nine months or 15 months or two years?

Can you offer anything to help out this committee in terms of why a year was picked?

● (1640)

Shannon Hiegel: As I mentioned earlier, we have done a lot of country comparisons within our analysis. One year was actually quite common in being the average. As I said, Australia is on the higher end, with two years.

We also want to make sure that we're clear that what we are expecting to retain within the metadata context still needs to be defined. The expectation is that there is some level of rationale. Maybe the metadata of me speaking with Fenton is really important, because now I know who was talking to whom, so it would be kept for a year, while something around—

The Chair: I'm sorry to interrupt, Madame Hiegel.

We need to move to MP Housefather for five minutes, please.

[*Translation*]

Anthony Housefather (Mount Royal, Lib.): Thank you, Mr. Chair.

[*English*]

It's always fascinating to listen to my colleague Mr. Caputo.

First of all, let me start by saying thank you so much for being here.

Obviously, I'm strongly in favour of this bill. As I said in the House, I think we need a modern access regime. I think we need to deal with Bykovets and Spencer and have proper legislation that allows us to deal with things like that.

I also had a couple of questions, if that's okay, with respect to the way systemic vulnerabilities interplay in this bill, in proposed subsections 5(5) and 7(5) of the bill versus proposed sections 12 and 13. Basically, what I understand from proposed subsections 5(5) and 7(5) of the bill is that a provider is not required to comply if a systemic vulnerability would be created. I think I have that right. However, proposed section 12 says, "An electronic service provider that is subject to an order made under subsection 7(1) must comply with it." Then proposed section 13 specifies that orders take primacy over the regulations that will be made.

I don't really understand, personally, the interplay here, where we're saying that somebody is not required to comply if it creates a systemic vulnerability, but then if there's an order, they're required to comply with it, and then the order supersedes regulations.

Can you talk me through this so that I understand how 5(5) and 7(5) actually work?

Shannon Hiegel: Sure. I'll start off, and then I'll turn to my expert, Fenton.

We have to consider this as a bit of a continuum, where the baseline has to be that you as a core provider—if it's regulation or if you're being tapped through a ministerial order—need to comply with this. Then there is the exception. If, as we go through this process with you to determine how to get that information off your networks, it is determined that it is a systemic vulnerability, then there is the right for a company to push back and say, "No, we can't give you the information you need because of a systemic vulnerability."

Anthony Housefather: If we want to say that, why would the bill itself not...? Right now, we agree that an order is paramount, and they must comply with the order. Is that correct?

Shannon Hiegel: Yes. That is the baseline.

Anthony Housefather: If the company believes that it would create a systemic vulnerability, under what circumstances is the company then able—unless it convinces the minister or representatives of the minister—to push back and say, "No, this would create a systemic vulnerability"? How come the bill as drafted doesn't say that the order must be complied with except to the extent that the company believes that, using reasonable commercial efforts, it cannot do this without creating a systemic vulnerability, or something like that?

If the company believes this, but the minister's office is not accepting that argument, what happens to the company?

Shannon Hiegel: Within the context of a ministerial order specifically.... I'll stay away from those who are—

Anthony Housefather: I'm only asking about the ministerial order.

Shannon Hiegel: Okay. The expectation is that Public Safety would be responsible for actually completing the analysis that the minister considers. Therefore, we intake information from the operating agency that has flagged the issue or the threat existing within a company's system. We actually are required to consult with that particular firm and satisfy a number of factors that are listed in the bill. As the company is with us through this process, they are able to voice their views.

Once we get to the final stage, if the minister then approves the process, the intelligence commissioner has full disclosure of all the information the minister had, and if he also agrees with the process to advance, the company does have the right to a judicial review.

● (1645)

Anthony Housefather: At what point? The company is told at that point that the minister and the commissioner have said they must go forward, regardless of their claim. Then they would go to judicial review.

What happens until that review is heard? Are you saying there would be a stay on carrying out the order?

Shannon Hiegel: That's correct.

Fenton, do you have anything to add?

Fenton Ho: No, I don't have anything to add.

Anthony Housefather: I appreciate that.

The Chair: Unfortunately, there is no more time.

Thank you, MP Housefather, for this intervention.

We will now move to MP Caputo for five minutes, please.

Frank Caputo: Thank you.

I want to pick up on the one-year retention period. If I understand it correctly.... The metadata is generally what we're talking about here, or whatever is contemplated in proposed section 5. Let's just say it's data that can be compelled to be kept. My understanding of what was said before is that one year is the maximum, and one year was chosen because it's like an international standard. There's nothing magic about one year. I understand that. Every number is arbitrary. However, not everything will be kept for one year. Am I clear on that?

Shannon Hiegel: Yes, that's correct.

Frank Caputo: Who decides what type of metadata will be kept for how long? Say, this type of data, an IP address or whatever, only needs to be kept for six months. Who decides that?

Shannon Hiegel: That will be achieved through the regulatory process, for which we will develop an analysis with the agencies as to what is most valuable when it comes to the investigative processes, as well as with companies. When we carry out the regulatory process, we have to consider things like the cost to industry of implementing new regulations. They would definitely be involved. As Rick mentioned, sometimes they already have that data in their holding, and there is no new delta cost to them. In other cases, it may be significant. We need to take the time to do that analysis and come back with a thoughtful scheme.

Frank Caputo: On first blush, I have an issue with that, because you only have to consider costs; you don't have to make your decision based on cost. It is a consideration.

The other issue is that one of the principal discussion points surrounding this bill is how much is left to regulation. Essentially, 90% of this bill could operate on regulation with ministerial orders and things like that. Should we not be spelling things out more in the bill when it comes to certainty? If you're a small electronic service provider trying to implement part 2, wouldn't you be shaking right now and thinking, “Oh my gosh, how much is it going to cost me to comply?” There is no certainty regarding what they'll have to comply with.

Shannon Hiegel: Let me tackle the last part of your question right up front. Core providers are also expected to go through a process by which we look at considerations of things like how big they are or how many customers they serve. It is unlikely that we would be regulating small business owners and operators through the core provider portion of this bill.

Frank Caputo: Again, I'll go back to my prior point. That falls to regulation and it falls to somebody else's decision where there is a consideration about the size and the cost. Ultimately, just because it is considered, that doesn't mean the core provider won't have to do what a ministerial order says. Does that make sense?

Shannon Hiegel: I understand what you're saying. Part of why the bill has a higher level of detail than others you may be thinking of is the fact that it is heavily based in technology. Using terms that could be obsolete within a number of years would render the whole bill useless.

● (1650)

Frank Caputo: I appreciate that. I know that some things have to be left to regulation. My view is that a bill like this should be as prescriptive as possible, where it can be, because there is so much left to regulation.

For instance, every ministerial order, as I see it under proposed section 7 in part 2, has to be approved by the intelligence commissioner. Is that accurate?

Shannon Hiegel: That's accurate.

Frank Caputo: Why not a Federal Court judge? I get it. They're both presumed independent. I assume the intelligence commissioner is presumed independent; I can't imagine why. Both are government-appointed. Both are presumed to have perfect knowledge, and I think you know what I mean by perfect knowledge. They are both presumed to have all the knowledge. A Federal Court judge, however, is not beholden to the government. They aren't “hired”. Their term isn't renewed or anything like that. They can sit until they're 75.

Why not have a Federal Court judge play the role of gatekeeper, rather than the intelligence commissioner, when there is at least a reasonable perception of connection to government?

Shannon Hiegel: Before I flip it to Fenton, I just want to say that within the ministerial order process, we have the Department of Public Safety doing the analysis. We have the minister approving. We have the intelligence commissioner, who is independent, also approving. We have a quasi-judicial oversight body, and then there can be a judicial review. Literally, on the judicial side, that's the only entity we've left out.

Fenton Ho: I would add that, at the end of that, we have NSIRA.

I think the intelligence commissioner is well versed because they are used to doing lots of things like ministerial authorization for CSE and the justification framework for CSIS. They're well versed in these particular issues. They have the knowledge, and from that point, they can actually do that function well.

The Chair: Thank you.

I'm sorry, MP Caputo. We have run over the time.

We are going to suspend now, since, as we have seen, the minister has entered the room.

Thank you, officials. Many of you will stay.

[*Translation*]

We will resume the meeting in a few minutes. The meeting is suspended.

● (1650)

(Pause)

● (1655)

The Chair: I call the meeting back to order. Thank you, everyone, for coming back.

I'd like to welcome the two ministers and the officials accompanying them, starting with Minister Gary Anandasangaree, MP and Minister of Public Safety. I would also like to welcome Minister Sean Fraser, MP and Minister of Justice.

Welcome to both of you, ministers. We'll begin with an opening statement from the Minister of Public Safety, followed by the Minister of Justice.

Mr. Anandasangaree, you have the floor.

Hon. Gary Anandasangaree (Minister of Public Safety): Thank you, Mr. Chair.

[*English*]

I would like to start by acknowledging that we're meeting on the traditional and unceded territory of the Algonquin Anishinabe people.

[*Translation*]

Thank you for inviting me to appear today to speak about the proposed Bill C-22.

[*English*]

I also want to acknowledge my colleague, the Honourable Sean Fraser, as we've been working on this bill for a number of months, and also the officials who are here to support us.

As Minister of Public Safety, my top priority is to ensure that every Canadian remains safe and secure. Since my appointment, I've heard clearly from law enforcement at all levels—municipal police services and the RCMP—as well as victims groups such as the Canadian Centre for Child Protection. They've all said that Canada needs modern tools to take on the wide array of illicit activities that are facilitated by the global digital environment.

Technology has fundamentally changed the nature of crime and threats globally. Criminals are continuously exploiting the digital space we all use, in order to facilitate a wide array of offences. This includes extortion, childhood exploitation, auto theft, terrorism and human trafficking. Furthermore, this environment is being used to facilitate foreign interference and violent extremism.

Our laws have simply not kept pace with our digitally driven world. This has created a significant gap between today's crimes and threats and what our current laws can meaningfully address.

[*Translation*]

We have a duty to Canadians to address these new threats.

[*English*]

This is what Bill C-22 aims to do.

It's worth taking this opportunity to highlight that Bill C-22 does not aim to regulate the Internet, police activity on the Internet or require Internet service providers to become agents of the government, as some of the debate in the House has suggested.

As our officials have confirmed, Bill C-22 is encryption-neutral. It is simply to address gaps in our legal framework that present challenges to timely access to information and intelligence that are vital to conducting investigations. It will give our officers the tools they need to keep Canadians safe in the 21st century, while ensuring we continue to uphold Canadians' charter and privacy rights.

● (1700)

[*Translation*]

We listened to the concerns of stakeholders and other parliamentarians after the tabling of Bill C-2.

[*English*]

Part 1 of Bill C-22 includes important safeguards, such as limiting the scope of confirmation of service demand to telecommunication service providers; a narrow definition of subscriber information; and strong judicial oversight. Police will still require court approval to obtain personal details like names, addresses and phone numbers.

Under part 2 of the bill, we'll ensure that electronic service providers can fulfill lawful access requests. Let's be clear: This part does not create new authorities for law enforcement agencies and CSIS to intercept communications or obtain information. Its focus is to ensure that electronic service providers are able to comply with existing legal orders, which are found in the Criminal Code and the Canadian Security Intelligence Service Act. Key elements include a new compliance framework that will require core providers to have the technical capability to comply with legal authorization to obtain information, such as warrants and production orders.

It would also give new ministerial order powers to the Minister of Public Safety. Only with approval from the intelligence commissioner, the minister could order an electronic service provider to develop specific technical capabilities: for example, to address new technologies that are developed but not captured in the regulations.

Finally, it introduces regulatory enforcement tools, such as administrative monetary penalties for any provider that does not comply.

Once again, I wish to underscore the safeguards that would be in place under this part of the bill. As I mentioned, all ministerial orders will require prior approval from the intelligence commissioner to ensure they are reasonable.

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.

We want Canadians to see exactly how these powers are being created and used to ensure that their implementation is subject to the highest levels of democratic scrutiny. Under our current laws, our police and intelligence officers are trying to fight tech-savvy criminals and state actors with tools that are decades old. Bill C-22 would bridge that gap, while upholding the charter rights and the privacy of all Canadians.

[*Translation*]

Thank you. I look forward to your questions.

The Chair: Thank you, Minister Anandasangaree.

Minister Fraser, the floor is yours for five minutes.

Hon. Sean Fraser (Minister of Justice): Thank you, Mr. Chair.

Before I begin my opening statement, I'd like to thank everyone for being here to take part in this very important debate.

I think it's important to understand the context of this bill. To improve public safety, we have a strategy built on three pillars. The first is to strengthen criminal laws, particularly with Bill C-9, Bill C-14 and Bill C-16.

That said, we recognize it's not enough just to make changes to criminal laws. We also need to support those working on the ground in our communities, such as community organizations and police officers. It's not enough to increase the number of people working in the communities. We also have to give them the tools they need so they can meet the expectations we have for the officers on the ground.

We also need to invest to prevent crime and violence in the long term. That includes making investments in affordable housing, making investments so people with mental health issues can have medication and making investments to support young people who have issues in their lives.

[*English*]

This bill is focused on that second pillar, supporting those who are on the front lines trying to make Canada safer every day. We can't expect people to address modern challenges with outdated technologies. That's where this bill comes in.

When we compare Canada with other partners around the world, we are significantly behind when it comes to addressing modern challenges, particularly in a digital context. Technology has changed. The world has changed. Crime has changed. It is faster-moving. It crosses borders. It is digital on an increasing basis. We've seen that other jurisdictions have embraced what we are discussing and calling “lawful access”. Very simply put, it's the ability of law enforcement to get access to the evidence they need that may be digital in nature, the same way we would allow them to get access to evidence that exists in the physical world. You can't arrest an IP address or a phone number.

We need to give tools to ensure that law enforcement has the ability to figure out, where there is a criminal investigation going on, who is the person behind it and how they can advance that investigation. When I look at the actual process we've laid out, I think it's important that we demonstrate to Canadians that we have put significant thought into ensuring that privacy rights are protected, in the same way that we embrace the recommendations of law enforcement to make it easier for them to do their jobs.

In particular, to start off, what we're allowing under this legislation is for law enforcement, when they have an investigation involving a phone number or an IP address, to make a simple request of a service provider: “Is this on your network?” If the network comes back and says it is, that would allow us to move forward with a process, which would be approved by a judge, to say, yes, there is a person with a name and an address attached to this. Currently, this process can take months. When we're dealing with people who are involved in criminal organizations—engaging in child sexual exploitation, engaging in drug trafficking and human trafficking, organizing home invasions and auto theft rings—you can appreciate the need to move quickly. It is essential if we're going to reduce the ultimate consequences of crime to Canadian communities.

This bill, in my view, provides the appropriate framework that empowers law enforcement to have the tools they need to keep Canadians safe, but it puts protections in place to ensure that, where appropriate, judicial authorization remains essential, and we put a system in place so that service providers actually do hold the information that will help facilitate these investigations.

Let me perhaps sum it up simply: We are not going to solve Netflix problems with Blockbuster technology. We have to join the advanced economies in the world that have been working to solve these problems for many years. With the support of different parties at this committee, I think we have the potential to send a strong signal to Canadians that when it comes to public safety, we will make absolutely sure that law enforcement has the tools they need to keep Canadians safe.

● (1705)

[*Translation*]

Thank you, Mr. Chair.

The Chair: Thank you, both.

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

[*English*]

Frank Caputo: Thank you, Mr. Chair.

Thank you to the ministers and officials.

I'll note that we have two Kamloopsians at the table today. That's always wonderful.

Minister Anandasangaree, you're off the hook today. We won't be asking you about visas and who gave people from the IRGC a visa. We'll stick to Bill C-22 here.

I want to go into something you mentioned, Minister. You talked about this being encryption-neutral. One of the greatest concerns I'm hearing about is encryption. Please don't defer to the analysts. I want to hear your perspective on this. This bill could threaten encrypted communications, based on the way it is written or the way some people are reading it.

Can you confirm that the purpose of this bill is not to go after end-to-end encryption, as in party A is using a program to deal with party B that is encrypted and there's no way to decrypt it? Can you confirm that this is neither in this bill nor the intent of this bill?

Hon. Gary Anandasangaree: I can confirm that, yes.

Frank Caputo: I'll just ensure one step further: that there's no requirement for company A, then, from point one to point two, to create what some would call a back door, a mechanism by which that information can be accessed. Is that accurate as well?

Hon. Gary Anandasangaree: I addressed that in my initial opening.

Frank Caputo: If there's any ambiguity on that, I trust you would support an amendment to close that, because this is a game-changer when it comes to that bill.

I take that to be the case.

Hon. Gary Anandasangaree: I would say what I told you privately, Mr. Caputo. We brought this bill forward with a number of engagements, including with colleagues in different parties. We will work in collaboration to strengthen the bill. If there are specific recommendations that this committee comes up with, we will certainly take them under consideration. We look forward to that engagement to get to the right result.

● (1710)

Frank Caputo: I'll be blunt, Minister. The Liberal government now has a majority. There is a concern that, if there is room there, it won't be addressed.

That's why I'm asking you, on the record, if there's a chance that encrypted communications can be targeted by this bill. If that's not the intent of the bill—that's what you said—I don't think it's too much to say, “Yes, Mr. Caputo, I would support an amendment to ensure that our intent is clear.” For instance, that could be an amendment that includes a definition of encrypted data in part 2 or an amendment that says that “systemic vulnerability” includes a key to encrypted data and the creation thereof.

With all due respect, Minister, I don't think it's difficult to say, “Yes, that's our intent.” Do you not agree?

Hon. Gary Anandasangaree: What I will repeat is that we are willing to work together in collaboration in advancing the bill.

I was at the Senate yesterday on Bill C-8, and 75% of the amendments that were passed were opposition amendments. They weren't government amendments.

On this bill, I think we have been very clear, both of us, that we will work with the opposition, as we have on every other bill, to advance and strengthen the bill.

Frank Caputo: The difference with Bill C-8, though, Minister.... If you want to get into Bill C-8, that is exactly my cautionary tale. The Liberals voted against just about every amendment that was of consequence. It was the Conservatives and the Bloc that voted for those amendments, that swayed those amendments, with the government often voting against them. Now things have changed. With all due respect, Bill C-8 is not a great example to use. That's why I'm trying to get it on the record.

I think I've made my point. You've made your point. Let's move on.

The ministerial order is one of the biggest things. One of them, as I said, is encryption; another major issue is the degree to which enforcement and definitions are left to regulation. That's one of the primary criticisms of this bill.

I look at proposed section 5, for instance. This is sweeping powers. Proposed paragraph 5(2)(b) says, “the installation, use, operation, management, assessment, testing and maintenance of any device”. Proposed paragraph 5(2)(d) says, “the retention of categories of metadata”. Minister, I get why the government wants things to be broad; it's because then you can account for things. However, should we not be defining things where we can define them? I'm pretty sure we're going to have experts who say, “Do you know what? We can define categories of metadata.” I'm sure we can define categories of metadata. Those don't change every day.

Would you be open to an amendment that says that when we're looking at taking information from people over which there's a high expectation of privacy...? I trust you would support an amendment that would define those types of things.

Hon. Gary Anandasangaree: I'm going to go back to my initial position, Mr. Caputo. We will consider specific amendments that you propose. I will personally engage with you on this. However, I don't think I am going to pre-emptively agree to amendments that you're proposing here.

Frank Caputo: Just [*Inaudible—Editor*].

Hon. Gary Anandasangaree: It would be irresponsible for me to say that I will accept all of these amendments. I think what's important is that we look at them and at the implications for the bill. We'll be more than glad to give you our feedback—as I always have.

The Chair: Thank you for that respectful and useful exchange.

Madame Sodhi, you have six minutes, please.

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

Thank you to our ministers for attending today.

Minister Anandasangaree, in Brampton, we have seen a concerning rise in crime of any and all types, from car thefts to robbery, breaking and entering, murders and shootings in broad daylight. I'm worried about the safety of my constituents and all residents of Brampton, and they are as well. Our mayor, Patrick Brown, and Peel Regional Police chiefs have been calling for legislation like Bill C-22 and have welcomed this bill's introduction.

With that local context in mind, can you describe the specific threats this bill is designed to respond to and the real-world operational gaps facing law enforcement and CSIS today that Bill C-22 would close?

● (1715)

Hon. Gary Anandasangaree: Let me acknowledge the work of Peel Regional Police in informing us on the development of this bill. It's been quite critical. I've had conversations with Chief Nishan Duraiappah on a number of occasions.

This is the number one priority as indicated by police leaders, not just in Peel, but across Canada at every level, whether it is Commissioner Carrique in Ontario with the OPP or Commissioner Duheme at the RCMP, as well as regional police services. This is of critical importance.

In a granular sense, the technology we have today is inadequate to deal with the types of issues we're dealing with. Primarily, telephones, the Internet, emails and electronic devices are used on a day-to-day basis for the execution of crime. Extortion, for example, is oftentimes done by way of a phone call or a text, or sometimes by email. Over the years, all of this has meant a great deal of delay for law enforcement to be able to get production orders. Oftentimes, they have to wait weeks, sometimes months, to get the information that will enable them to go to the next step.

Essentially, what we're doing here.... I'll use the example of a phone directory or Bower's reverse lookup, which can be found at a local library. If you have a phone number, you can go to the Bower's directory, put the phone number in and get the address of the individual who owns the phone number. Right now, these are often anonymous, which means that we need to go to the service provider. If it is a telco, we need to go to the telco and ask if this particular telephone number is associated with their service. It takes weeks, sometimes months, to get that information.

Bill C-22 would, as a starting point, enable law enforcement to get what's called confirmation of service. That will say whether this phone number is attached to the service the telco provides. Once that information is obtained.... It's a yes-or-no answer. If it's a no, the matter stops there. If it's a yes, then a production order, a warrant, will need to be prepared, seeking subscriber information on the individual whose phone number may be associated with the telephone company. Based on the warrant, we will get basic subscriber information, which would be their name, email address and so on.

Beyond that, any additional information that is required will go back to what we do right now, which is go back to court, all under judicial authorization, to be able to get the type of information that's required for that investigation to continue. Essentially, an investigation that takes months could take weeks, based on the additional provisions that are provided within this bill.

Amandeep Sodhi: Minister, you said that you discussed it heavily with Chief Nish from Peel Regional Police. Do you find there is consensus? Do police jurisdictions from all over Canada want Bill C-22?

Hon. Gary Anandasangaree: I would say that we've had a number of engagements. The Honourable Murray Rankin engaged in some mediation sessions and advised us on near consensus. I wouldn't say there was consensus, but there were civil liberties organizations and industry representatives present. We had law enforcement, as well as community advocates in different conversations.

What we have here is an area where I think there is a great deal of understanding and acceptance. It is not perfect. Not everyone is 100% behind this. There are concerns that people continue to express, but, by and large, this reflects.... Even with law enforcement, we have had to curtail.... You will see some significant changes in Bill C-22 from Bill C-2, for example narrowing and defining certain aspects of what is included.

We have done an enormous amount of work to build what we think is as close to a consensus as we can get. We won't get full consensus. I think the work we need to do is make sure that all the safeguards are in place. We are fully confident that both privacy and charter rights concerns are addressed in this bill. Some would like us to go further. Some would like us not to have a bill whatsoever, but that is not an option for us.

● (1720)

The Chair: Thank you very much for that, MP Sodhi.

[*Translation*]

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

Claude DeBellefeuille: Thank you, Mr. Chair.

Thank you very much, ministers.

Mr. Fraser, I don't really have any questions for you, but I honestly want to congratulate you on your French, which has greatly improved.

Mr. Anandasangaree, the Support for Authorized Access to Information Act, enacted by part 2 of the bill, provides for a limited role for the National Security and Intelligence Review Agency, the NSIRA. However, we've noticed that there are comparable legal access mechanisms among our Five Eyes partners that come with a more formal independent oversight role. Australia is an example, where the Telecommunications and Other Legislation Amendment (Assistance and Access) Act of 2018 mandates the NSIRA's counterpart be notified of the issuance of technical assistance orders within a specified period of time.

According to Bill C-22, a year later, you have to provide the agency with an unredacted report, and, if I'm not mistaken, you have 90 days to do so. This means you're handing this report to the review agency about a year and a half after the fact or after the decisions were issued.

You've drawn inspiration from the Five Eyes for your bill, so why don't you want to give the agency a role as important as the one given by Australia to their oversight body?

Hon. Gary Anandasangaree: Thank you for the question.

[*English*]

I would say that there are a number of safeguards that have been built into Bill C-22. For example, on ministerial orders, there's a requirement to get acceptance from the intelligence commissioner before an order can be issued. There are provisions for judicial review in certain circumstances. There's also a reference to NSIRA *post facto*, and this is the ordinary review process—

[*Translation*]

Claude DeBellefeuille: I'm sorry to interrupt, but I've already read that. I came prepared.

I find the Canadian agency is somewhat sidelined and I'd like to understand why. I know the intelligence commissioner has a role, but why isn't the agency notified in real time? It's hard to conduct an investigation into whether the agencies involved, such as the RCMP or the Canadian Security Intelligence Service, are complying with the law when you get the facts almost a year and a half later.

I'm letting you know I'll be proposing an amendment so the review agency is notified in real time, similar to the Australian model, because I think that's our guarantee. It's a bit like entrusting the government by ensuring the review agency, whose primary mission is to conduct oversight, is notified in real time, like the intelligence commissioner.

I was also surprised to learn from your team that the various consultation groups organized to study Bill C-22 didn't consult Ms. Deschamps, the current agency chair. That doesn't make sense to me, honestly. We look to our Five Eyes partners for best practices, yet we fail to include an important role for the agency in Bill C-22. Would you be willing to discuss the idea of notifying the agency in real time?

[*English*]

Hon. Gary Anandasangaree: I would say, in part, that in order to move forward on a ministerial order, the timeline for it to go through the NSIRA review process could be quite significant, so this is a safeguard that's built in. The role of the intelligence commissioner, as you're aware, involves a lot more real-time responses and the ability of the intelligence commissioner to give that feedback. That safeguard is there so that the intelligence commissioner could approve or not approve a proposed order—

[*Translation*]

Claude DeBellefeuille: What prevents you from notifying the National Security and Intelligence Review Agency? That's what I don't understand. I don't understand why you're excluding it. Its primary mission is to monitor and you're setting it aside. It's only informed a year after the fact.

I'll repeat my question. I'll propose my amendment. I know you said in the House of Commons that you'd be open to amendments. If you're going to notify the commissioner, I don't understand why it's complicated to also notify the office of the agency's chair. I think it would make sense, and that's more or less what Australia's doing. However, you don't seem open to the idea. Do you have any arguments to convince me I'm wrong to ask you for this amendment?

● (1725)

[*English*]

Hon. Gary Anandasangaree: First of all, I did meet with the intelligence commissioner, the Privacy Commissioner and the chair of NSIRA. I have done a number of engagements on a personal level, on top of the engagements undertaken by our departments.

We don't believe NSIRA can provide, in a timely manner, the required acceptance or rejection of a particular ministerial order, just given the urgency of the matter in some cases. This is why the intelligence commissioner is being utilized in this regard. The role of NSIRA is always as a review, as a *post facto* review agency. This legislation is in line with the way NSIRA is currently operational, which is to review matters and to report back on potential errors, potential omissions—

[*Translation*]

Claude DeBellefeuille: I'm going to interrupt you, Minister.

You know the agency chair disagrees with your interpretation. She told us she thinks she should be notified. She might not need to give her authorization, but she should at least be informed when there are ministerial orders, just like the commissioner. They may not have the same role, but she could at least be informed. In that sense, I think it's important for the agency to have a more important role so it can earn the public's trust. That's my opinion.

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

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

[*English*]

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

Ministers, I appreciate your being here.

I appreciate what you say about supporting our frontline officers. Lawful access has been called for over many years. I do think, though, that we have to be careful not to rush something through. We need to get it right. We need to balance, as parliamentarians, our duty of care that we are protecting the privacy of Canadians. My questions will be based on that. I think we have to be careful not to race to royal assent. We have to do this right.

More than a decade ago—I don't know if you're aware of this—your party warned against a bill very similar to this. It was a lawful access bill. They said it risked turning Canada into a surveillance state. Today you are advancing similar powers, but actually in a more expansive form, with Bill C-22. In fact, Mr. Francis Scarpaleggia, our current Speaker of the House, was at the time the Liberal public safety critic. He warned that similar lawful access legislation, in his words, risked “creating an Orwellian service state”.

My question for you is this: Was he wrong?

Hon. Gary Anandasangaree: I will say that successive governments have failed to advance lawful access as a very important tool and framework that is required—

Rhonda Kirkland: Yes. I'm aware that it has failed to continue. My question is, has the Liberal government changed their position from what they had over a decade ago, or do you believe Mr. Scarpaleggia was incorrect at that time?

Hon. Gary Anandasangaree: I mean, this is not about Mr. Scarpaleggia, Ms. Kirkland. This is about the safety and security of Canadians. As you're aware, Canada's new government, under Prime Minister Mark Carney, undertook to ensure, as Minister Fraser aptly outlined, the three pillars. This is a very important part of that pillar.

Maybe Sean could add to this.

Rhonda Kirkland: I'm going to move on. I'll get to questions for Mr. Fraser momentarily.

Minister Anandasangaree, can you give any assurances that this legislation, as it is written, will not be used in ways that go beyond its original intent? I've heard department officials say that the bill is not intended to do X, Y and Z. However, if the bill allows the government to do those things, what is to prevent a future government, which maybe has an approach to privacy and civil liberties that's different from yours, from abusing that power?

Hon. Gary Anandasangaree: I will say that a lot of thought has been put into ensuring that the safeguards are in place, both from a privacy perspective and to ensure that it is charter-compliant. We are very confident that the bill as presented does have those safeguards.

Rhonda Kirkland: At the time, over a decade ago, when we tried this, there were warnings that rushing complex surveillance laws without properly gauging Canadians' views could lead to failure. You mentioned that you were very confident that privacy and safety are addressed in the bill as it is currently.

Your government relied on consultations led by Murray Rankin to inform Bill C-22, yet you have not released that report. Will you release Mr. Rankin's report and share it with this committee?

● (1730)

Hon. Gary Anandasangaree: I would say that Mr. Rankin's report—and I'm grateful for the work he has done—was prepared.... He is a lawyer. We are both colleagues. It was presented to me—and Mr. Fraser has used it through me—to inform our decisions.

The bill right now is not about Mr. Rankin's report. What I would say is—

Rhonda Kirkland: Sir, I just wanted to ask, is that a no, then, that you will not release the report to the committee, or yes, you will?

Hon. Gary Anandasangaree: I'm seeking privilege on that matter. I don't believe that will be released, no.

Rhonda Kirkland: Over a decade ago, the Liberal government warned that government rhetoric shut down meaningful debate on that iteration, Bill C-30's lawful access provisions, yet today this committee is being asked to study similar powers without access to the consultation report that informed how to proceed with lawful access reform in Bill C-22. That report is essential to any meaningful scrutiny and Parliament's ability to do its basic legislative function. By withholding it, your government is effectively asking MPs to approve legislation without full disclosure of the evidence behind it.

Why, sir, are you refusing to release this report, while insisting that we move forward with these powers?

Hon. Gary Anandasangaree: I would say—

Rhonda Kirkland: Why are you insisting?

Hon. Gary Anandasangaree: If I may answer, Ms. Kirkland—

Rhonda Kirkland: Thank you. I want you to just answer that question, though.

Hon. Gary Anandasangaree: You had a preamble. I should be able to give you a wholesome response.

If I may, what I would say is that, in the normal course of bringing a bill forward, there are a number of different pieces of information that a department relies on to develop the legislation and get the requisite authorities in order to bring forward legislation. The vast majority of the time, none of this information is disclosed. That is part of the decision-making of the government.

You're welcome, Ms. Kirkland—

Rhonda Kirkland: The difference between the Five Eyes and our country is that we have a charter—

The Chair: I'm sorry to interrupt both of you.

We now need to turn to MP Casey for five minutes, please.

Sean Casey (Charlottetown, Lib.): Thank you very much, Mr. Chair.

I was in Parliament the day Francis Scarpaleggia went after Vic Toews with respect to the lawful access legislation at the time, and I distinctly remember Minister Toews saying that either you're with the government or you're with the child pornographers. I remember the proliferation of the hashtag “TellVicEverything”, because there was a widespread perception at the time that the legislation was an overreach. Right across the country, there were people who were providing Minister Toews with information about spilling soup on their tie, because they felt that perhaps Vic was interested in everything, with the measures he was taking to trample privacy and the over-the-top rhetoric that was being used at the time to support it.

I'd like to bring Minister Fraser into the conversation.

Minister, in your opening remarks, you talked about the protection of privacy and compliance with the charter in that regard. Can you talk a bit more about the protection of privacy and the compliance with the charter and the efforts that have been made in this legislation on the two?

Hon. Sean Fraser: Look, to help us get there, I want to provide a bit of context.

Ms. Kirkland, when she led her questions, talked about this debate going on for a few years. It hasn't been going on for just a few years; it's been going on for 30 years.

I invite everybody to watch the video of Commissioner Carrique's summary of the importance of this bill upon the legislation being tabled. You can hear the frustration coming out of law enforcement. I think there is consensus among law enforcement to move forward, because they are very tired of the criminal organizations responsible for human trafficking, auto thefts and drug trafficking. They know this activity is going on, and they are trying to do their jobs with one hand tied behind their backs. When they receive tips from foreign governments, in particular, on something as sensitive as child sexual exploitation, they want to move. They do not want to invade people's privacy along the way.

Thankfully, there have been several evolutions in Canada and around the world that demonstrate how we can better protect privacy. There's been some discussion at this committee about the differences between the approaches of our Five Eyes partners and Canada's. Of our Five Eyes partners—or France, Germany, Finland or Spain, for that matter—none require judicial authorization to get subscriber information. We're talking about information that used to be in the phone book. We would still require that a court approve access to that information. This would streamline access without compromising privacy in any significant way.

If you want to go beyond that, even in exigent circumstances.... The one exception would be when an emergency is playing out and the crime can be stopped, or if evidence is going to be destroyed. There would even be opportunity on the back end to.... The test would still have to be met, but the harm could be undone, so to speak, by a court excluding evidence, should they need to—if, in fact, there was a privacy breach committed.

We've improved this, by the way, through a consultation process with different MPs from different parties, and with experts who said, “You know, you might want to ring-fence what subscriber information you're looking for”, so we excluded medical information and legal advice. This is about finding out who is behind a phone number or an IP address when we suspect they are tied to a criminal activity of one kind or another.

At every step of the way, we've tried to give law enforcement the tools they need to combat modern crime. At every step of the way, we've said, “How are we going to do this in a manner that respects the reasonable expectation of privacy protected by the Canadian Charter of Rights and Freedoms?” I'm convinced that we found the right balance, after many years of debate and many months of discussion among parliamentarians of different parties. This strikes a balance that will allow us to defend the interests of Canadians, keep our communities safe and respect the privacy rights of Canadians at the same time.

● (1735)

Sean Casey: Minister Anandasangaree, do you have anything you'd like to build on, based on the answer you just heard?

Hon. Gary Anandasangaree: I think Minister Fraser has captured the work we've done, and the urgency.

What I want to underscore is this. As technology develops and emerges—we know we're already 30 years behind in this work—in terms of AI and other tools at a scale and speed that I don't think our world is quite ready for, the need for a lawful access framework in Canada is essential, at the very minimum, to keep us up to date and evolving.

The Chair: Thank you very much for that.

[*Translation*]

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

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

Minister, you told Mr. Caputo the intent behind Bill C-22 isn't to create back doors in encryption systems, now or in the future. You've confirmed that.

The possible weakening of encryption was also a concern for us when we studied Bill C-8. At the time, Minister Joly told us that even if the bill expressed a certain intention, she would agree to add a clause clearly stating that encryption will not be weakened.

Honestly, the weakening of encryption is really a widespread fear. Perhaps you could reassure the public by making it clear in the bill that you will not undermine encryption systems.

Do you think there's room in the bill to further clarify your intention, since you told the previous speaker it wasn't your intention to weaken encryption?

[*English*]

Hon. Gary Anandasangaree: As I indicated, we will look at every amendment. There is an amendment-making process. Once you complete the work, there will be recommendations coming forward from the committee. The undertaking I can give you is that we will look at every single one of those proposals and give you feedback. As always, I will engage with you, Mr. Caputo and others who want to advance on this issue.

That's the commitment I can make to you today.

[*Translation*]

Claude DeBellefeuille: Minister, when Minister Joly appeared before the committee, she committed to having the government table an amendment to Bill C-8 to add that there would be no weakening of encryption. She said so publicly during the study on Bill C-8.

I'll ask you the same question, then. To reassure the public, are you prepared to ask your team to state in the bill that there will be no breaches of encryption systems?

● (1740)

[*English*]

Hon. Gary Anandasangaree: I have worked with you very closely now for almost a year, and I think you generally know the approach that I have taken in collaboration. I am certainly willing to meet with you and look at the proposal you have.

We would be more than glad to entertain anything to strengthen the bill.

[*Translation*]

The Chair: Thank you, Mrs. DeBellefeuille.

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

[*English*]

Dane Lloyd: Thank you, Mr. Chair.

Thank you to the ministers for being here.

Minister, you've refused to waive privilege on the report provided by Murray Rankin, on the consultative process in this report. I've been told that this report has been widely shared with people who have participated in the consultation. I'm assuming that those people who have not shared the report have done so because they signed a non-disclosure agreement.

Can you confirm if the members of the consultation had to sign a non-disclosure agreement in order to get access to the report?

Hon. Gary Anandasangaree: Mr. Lloyd, I'm not sure if they did or not.

The conversation today is not about Mr. Rankin's report; it is about the bill that is in front of the House. There is no precedent for governments to be sharing information that was gathered and discussions that took place with a committee. I think we're sidestepping the core issue we're here to discuss, which is the bill itself.

Dane Lloyd: Thank you. I've given you enough time on that, Minister.

This report was critical in your government's coming up with the report. It would be very helpful for us, as members of Parliament, to have access to this report. I think it's critical that governments try to build trust with Canadians. I have to admit that what you're doing here, Minister, does not look accountable or transparent, especially when we're dealing with very contentious legislation that deals with the privacy rights of Canadians.

What are you hiding, Minister? Why are you refusing to share this report?

Hon. Gary Anandasangaree: You're welcome to call Mr. Rankin to the committee, and he will be able to provide information.

What is happening right now is a bit of a distraction from the core issue, which is discussion on the bill itself.

Dane Lloyd: Minister, you're making it a distraction by refusing to reveal the report. The fact that we're talking about it today.... Even people who received the report—people who support Bill C-22 and people who are against it—are baffled as to why this report hasn't been revealed.

It's becoming a distraction because you're making it a distraction, Minister. Why not just reveal the report?

Hon. Gary Anandasangaree: The matter is not about the report, Mr. Lloyd. You know this. This is about the bill itself, as presented by me and Mr. Fraser. If you have specific questions about the bill, I will be more than willing to answer them, but I'm not willing to answer you on privileged information that I believe I sought from Mr. Rankin, which informed our decisions.

There are also a number of other individuals with whom Mr. Fraser and I met. We consult a range of people on developing a bill—

Dane Lloyd: Minister, I've given you plenty of time to respond.

Why should the stakeholders who participated, such as the Canadian Civil Liberties Association and other stakeholders, have more of a right to see what is in this report than members of Parliament, who are being asked to vote on this legislation?

Hon. Gary Anandasangaree: If you would like to invite Mr. Rankin to testify, you're more than welcome to do so.

Dane Lloyd: I'm going to move on, Minister.

I was talking to your officials before. There seems to be a contradiction. The legislation says it's not intended to weaken encryption or create systemic vulnerabilities, yet there are other parts of the legislation that say a ministerial order is intended to create the very technical capabilities needed to get through this encryption.

If one of the outcomes desired by this legislation, that being lawful access, cannot be accessed without creating systemic vulnerabilities, will your government still order telecoms and other ESPs to create these encryption capabilities?

Hon. Gary Anandasangaree: As I said initially, this bill is encryption-neutral. It does not envision or anticipate the breaking of encryption in any way. The ministerial orders, as contemplated, will require the intelligence commissioner to approve them, which is part of the safeguards that are in place right now.

Dane Lloyd: In response to my question during debate regarding compensation for providers, you were pretty blunt. You said that as a condition of CRTC licensing, you expect companies to comply without compensation.

Is that an accurate depiction of what you said in the House?

Hon. Gary Anandasangaree: What I will say is—

● (1745)

Dane Lloyd: Was it accurate, yes or no?

Hon. Gary Anandasangaree: Mr. Lloyd, I don't recall.

Dane Lloyd: Okay.

Hon. Gary Anandasangaree: I have commented on this, so I can—

Dane Lloyd: You're saying no to compensation. Is that correct? Just be clear.

Hon. Gary Anandasangaree: What I will say is that this bill.... There is a world in which compensation is possible—

Dane Lloyd: Oh, okay.

Hon. Gary Anandasangaree: —but my view is that companies that are operating in Canada are good corporate citizens. Five Eyes countries do not necessarily pay—

Dane Lloyd: That's very different from the answer you gave in the House.

In what situations do you think compensation could be provided?

Hon. Gary Anandasangaree: At this point, I don't anticipate any particular situation. If there were extenuating circumstances where a company's financial position may be limiting, that would be a one-off consideration, but by and large, we do not anticipate compensation will be provided.

The Chair: Thank you, MP Lloyd.

Next is MP Acan for five minutes, please.

Sima Acan: Thank you, Mr. Chair.

I want to share some technical considerations regarding metadata for my colleagues to consider before proposing amendments that could significantly impact the effectiveness of this bill.

Modern criminal investigations, especially those involving child exploitation, human trafficking, extortion, organized crime and cybercrime, rely heavily on digital metadata to reconstruct events, identify suspects and map complex networks. These cases are often reported long after they occur, making historical data essential for establishing timelines and connections that are not immediately obvious.

It is therefore potentially risky to narrow the types of data retained. Different metadata types serve different investigative and IT functions: attribution, communication mapping and cross-platform activity reconstruction. If key categories are excluded, it can break the chain of evidence and limit the ability to link activity across systems and jurisdictions. From an investigative and digital forensic perspective, missing metadata reduces the ability to conduct pattern and network analysis, which is central to modern intelligence-led policing and cyber investigations. It can also weaken evidentiary completeness in court. Many serious crimes are reported long after they occur. If certain metadata categories were never stored in the first place, they cannot be recovered later, even with a warrant or a court order.

Mr. Chair, I ask my colleagues to please refer to this transcript of my remarks when considering any amendments related to narrowing the types of metadata or limiting the retention periods, as these changes could significantly weaken the effectiveness of lawful access.

My colleague Mr. Caputo raised concerns regarding not only the types of metadata but also the 12-month data retention framework outlined in part 2.

During my meetings with law enforcement officials, they clarified the general parameters. There remains a practical challenge when it comes to complex investigations. Many serious cases, such as child exploitation, human trafficking, organized crime and extortion, are inherently time-intensive and often extend well beyond six or even nine months due to their cross-jurisdictional and digital nature.

Could CSIS or the RCMP elaborate on the operational importance of data retention in supporting these types of complex investigations? Also, significantly, how does the availability and duration of retained data impact the ability of law enforcement to conduct timely and effective investigations in the digital context?

Thank you.

Nicole Giles (Deputy Director, Canadian Security Intelligence Service): The ministers are gesturing to me, so I'll take that as my cue.

I can give two examples, perhaps. One example could be that CSIS is trying to determine the movements of a terrorist group, and we've received a warrant to track a person of interest's cellphone. The electronic service provider did not have the necessary capabilities to track the device, so we're out of luck if there are not the capabilities to track the device. That is one of the key capabilities that would be provided under part 2, because it would require ESPs to develop and maintain location tracking capabilities, which are, quite frankly, standard in Five Eyes and European countries.

Another example could be that we receive information from a foreign partner who is carrying out an investigation outside of Canada where a few of the subjects of the investigation are associated with a Canadian phone number, and the foreign partner has further highlighted that the threat looks like it's about to move into Canada. We're able to confirm that the phone numbers were obtained through a reseller, but the reseller, quite frequently, neither maintains records of its sales nor tracks its clients' activities. Part 2 would bring that into play by having the resellers brought into the process, which would allow us to respond to those types of requests.

● (1750)

Sima Acan: Do I still have time?

The Chair: You have 30 seconds.

Sima Acan: Okay.

Bill C-22 makes an important legislative change clarifying that....

Actually, it's not going to be enough, Mr. Chair. I'm okay with that.

Hon. Sean Fraser: Mr. Chair, if there are 20 seconds left—

Sima Acan: Minister, do you want to add something?

Hon. Sean Fraser: If I can just add, these are not fictional crimes. If you actually talk to law enforcement officials, particularly on the second example.... A lot of people don't appreciate this, but law enforcement in Canada is receiving an ungodly number of tips about potential threats, including child sexual exploitation. The application of the law is inconsistent between provinces, because it's unclear about the regime of how we actually use digital evidence to investigate and prevent crime.

These are real threats to—

The Chair: I'm sorry to have to cut off a ministerial colleague, but it's over, unfortunately.

[*Translation*]

Thank you to the ministers for taking the time to prepare and travel to join us today.

Thank you to all the officials for doing the needed work.

We will now adjourn, and we'll see you on Thursday for other business.