HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

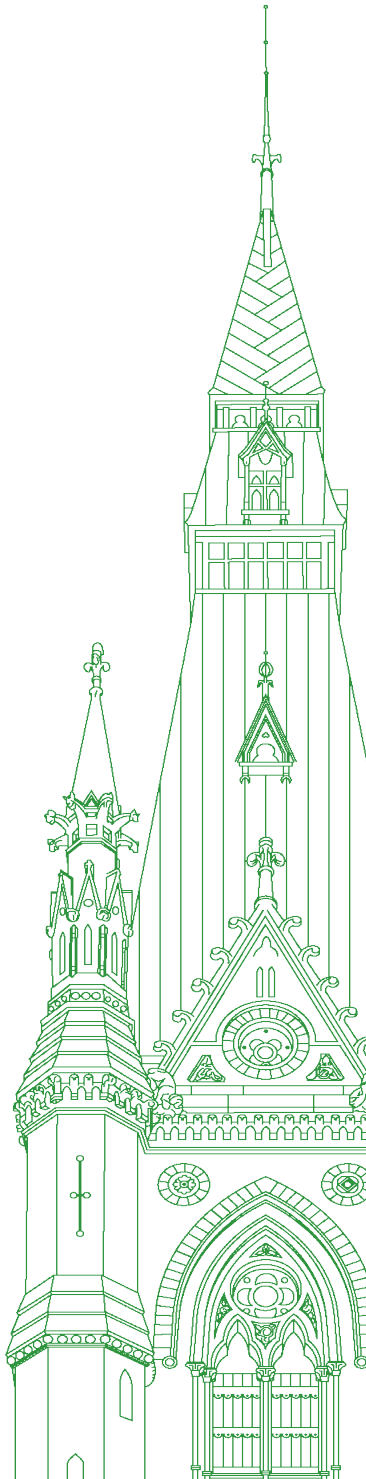
45th PARLIAMENT, 1st SESSION

Standing Committee on Public Safety and National Security

EVIDENCE

NUMBER 037

Thursday, May 7, 2026



Chair: Jean-Yves Duclos

Standing Committee on Public Safety and National Security

Thursday, May 7, 2026

● (1535)

[*English*]

The Vice-Chair (Frank Caputo (Kamloops—Thompson—Nicola, CPC)): I call this meeting to order.

First of all, it is a pleasure and an honour to be here as your vice-chair chairing this meeting. Thank you all so much.

Welcome to meeting 37 of the House of Commons Standing Committee on Public Safety and National Security. Pursuant to the order of reference of the House of April 20, 2026, and the motion adopted by the committee on April 30, 2026, the committee is resuming its study of Bill C-22, an act respecting lawful access.

Welcome to our witnesses.

We have Professor Leah West as an individual. We have the chief of police for Thunder Bay, Chief Fleury, and we have chief of police for the Toronto Police Service, Chief Demkiw.

Welcome to you all.

You all have five minutes to make an opening statement. For those in person, I will endeavour to get your attention when you're at one minute left and then when we're coming down to the end of your time. Hopefully I can do that as well for the people who are by video link.

With that, I invite Professor West to make an opening statement.

Thank you.

Leah West (Associate Professor, As an Individual): Chair and members of the committee, thank you for the opportunity to appear today.

By my count, Bill C-22 represents Canada's ninth attempt to enact lawful access legislation. That alone should give us pause. For over a decade, successive governments have recognized the same problem. Our laws have not kept pace with the realities of modern criminal and national security threats or the tools required to address them. The result is a growing gap between Canada's lawful access framework and the central role that electronic data plays in investigating and prosecuting crime.

At the same time, the Supreme Court of Canada has been clear that even basic identifiers can reveal deeply personal information and are therefore protected under section 8 of the charter. As the court recently reaffirmed, an IP address is often the first digital bread crumb that can lead the state on the trail of an individual's Internet activity.

The government and this committee have a difficult task to address the existing operational gap in a way that is consistent with the charter. Bill C-22 is a meaningful improvement over past efforts at reform. It reflects the hard work done by officials at Public Safety Canada to engage with stakeholders and revise earlier proposals. It is more carefully structured and, in my view, capable of getting us to a workable, lawful access regime, but it is not there yet.

Let me briefly highlight three areas where targeted amendments would significantly strengthen the bill.

First is the subscriber information production order. The bill introduces a new tool that allows police to obtain subscriber information on a reasonable suspicion standard. In my opinion, that standard is constitutionally defensible, but the bill as drafted goes too far in another respect. It requires service providers to produce all subscriber information, as defined, tied to an identifier, regardless of whether each category of data is relevant to the investigation.

This new power applies to anyone who provides services, not just telephone service providers, creating a risk of overcollection of private information that does not meet the legal threshold set out in the bill. The fix is straightforward: Amend the provision to give police the discretion to request and judges the discretion to authorize only specific types of subscriber information for which the standard has been met. If the standard for a production order is going to be suspicion, then the scope of what is authorized must be narrowly targeted.

Second is risk to individuals in foreign jurisdictions. The bill allows Canadian authorities to request data directly from foreign service providers. This power is important, but it carries risk. There is currently no requirement for a judge to consider whether such a request could expose the target to mistreatment in another country, and that is a gap. I recommend adding a clear obligation for judges to assess whether there is a substantial risk of mistreatment and to refuse the order where such a risk exists. This would align the regime with Canada's broader human rights commitments and what is already obligated for RCMP officers under the Avoiding Complicity in Mistreatment by Foreign Entities Act.

Third and most critically is part 2, or the SAAIA, which is what I'm going to call it. Requiring companies to build interception capabilities and retain data that they would not otherwise keep inevitably creates cybersecurity risks. Every additional access point and every new repository of data are potential targets. The question is not whether the bill creates new risks. It does. The question is whether the bill adequately mitigates those risks and strikes the correct balance between the risks and the public safety imperative. As currently drafted, I don't think that it does.

Three changes are essential.

First, strengthen the definition of “systemic vulnerability” and prohibit the GIC from weakening that definition through regulation.

Second, prohibit blanket data retention. I believe that the current authority engages the right to privacy, is overly broad and creates a significant cybersecurity risk. The current one-year framework departs significantly from existing 90-day preservation limits, and I've yet to hear a compelling argument for the need for a blanket retention obligation not tied to any specific collection authority or subset of offences such as serious crime. Any retention regime must be necessary for investigative purposes and must be reasonable and proportionate to the offence or threat under investigation.

Third, make explicit that law enforcement and CSIS cannot directly collect or intercept personal information or private information from service providers' systems. Control over access to providers' data and systems must remain with providers. They alone should flip the switch. This is critical for privacy, security and legal clarity.

● (1540)

In conclusion, I believe deeply that Canada needs lawful access reform, but the task is not simply to expand access. It is to ensure that any expansion is necessary, reasonable and proportionate, and that it does not undermine constitutional protections or create undue security risks for Canadians.

Bill C-22 is a meaningful improvement, but targeted amendments are still required to get this right.

Thank you.

The Vice-Chair (Frank Caputo): Thank you, Professor West. Your timing was perfect.

We will now move on to Chief Fleury, and you have five minutes. Thank you.

Chief Darcy Fleury (Chief of Police, Thunder Bay Police Service): Thank you, Chair and members of the committee, for the opportunity to speak with you today about Bill C-22, an act respecting lawful access, and why policing leaders across Canada strongly support its passage.

Policing in Canada has changed dramatically over the past decade. Crime is no longer confined to physical spaces or geographical borders. Today, organized crime networks appear across jurisdictions using encrypted applications, anonymous accounts and digital platforms to coordinate activities such as drug trafficking, human trafficking, firearms smuggling and cybercrime, yet the laws that govern how police access critical information were largely designed before the digital reality existed.

Bill C-22 is about closing that gap. It proposes practical, measured updates that would allow investigators to access certain information more efficiently, always with lawful authority, judicial oversight and a full respect for the charter and the privacy protections Canadians expect.

This is not about expanding unchecked powers. It is about ensuring that when police have lawful grounds to act—

The Vice-Chair (Frank Caputo): Excuse me, Chief. Could I interrupt you, please? Could you please take the boom of your microphone down just a shade so it's not touching your skin?

Chief Darcy Fleury: Okay.

How's that?

The Vice-Chair (Frank Caputo): Yes, I have a thumbs-up.

Thank you. I'm sorry to interrupt.

Chief Darcy Fleury: No, that's good. Thank you.

This is not about expanding unchecked powers. It is about ensuring that when police have lawful grounds to act, they can do so in a timely way, especially when lives are at risk.

We are experts in this area. Last year alone, the Thunder Bay Police Service investigated 184 cyber-related cases. This involved more than 140 production orders, 80 search warrants, and over 1,370 devices being seized for examination. These efforts led to 20 victims being identified, and more than 240 charges laid. This is impressive for a five-person unit.

However, this is not about statistics. It's about protecting people. Bill C-22 will help services like ours, facing increasing demands with limited resources, reach victims more quickly. Let me illustrate this in a more realistic scenario.

Imagine a missing 14-year-old girl: Shawna. Her parents report that she has been communicating online with someone they believe is exploiting her. Investigators identify a username linked to a messaging platform. Time is critical. Under the current framework, confirming which service provider holds that account information and obtaining the basic subscriber data needed to proceed can take valuable hours or even days due to fragmented processes and outdated legal pathways.

Meanwhile, evidence suggests the suspect may be attempting to move Shawna across provincial or international borders. Every hour matters. Under Bill C-22, investigators could more quickly confirm the service provider tied to the account and proceed with the appropriate judicial authorization to obtain further evidence. In urgent circumstances, they could request limited emergency access to data to prevent imminent harm, while remaining fully accountable to strict legal thresholds and oversight. That time saved could mean locating Shawna before she is moved, before further harm occurs and before critical evidence disappears.

This is the reality police services face every day. We have multiple examples in Thunder Bay where we have youth as young as 14 being exploited and coming to our community from southern Ontario. The Canadian Association of Chiefs of Police has endorsed Bill C-22 because it strikes the right balance. It streamlines access to essential information, improves emergency data sharing and clarifies voluntary disclosures, while maintaining strong judicial and privacy safeguards. The Ontario Association of Chiefs of Police has also consistently called for modernizing lawful access tools.

Our members see first-hand how individuals and organized crime group networks have exploited legislative gaps. These actors are sophisticated and constantly evolving.

To keep communities safe, policing must evolve as well. Lawful access tools are not about surveillance overreach. They're about public protection. They allow investigators to understand criminal networks, prevent violence and rescue victims. Whether it's locating a missing youth, disrupting fentanyl trafficking, dismantling human-trafficking networks or combatting online exploitation, clear legal frameworks and modern tools are essential.

Bill C-22 represents an important step forward. It acknowledges that modern crime requires modern solutions. It ensures police can act quickly in urgent situations, while remaining firmly grounded in judicial authorizations, privacy laws and the Charter of Rights and Freedoms. At its core, the legislation is about protecting Canadians, especially the most vulnerable among us.

I urge you to support the timely passage of Bill C-22.

Thank you.

● (1545)

The Vice-Chair (Frank Caputo): Thank you, Chief Fleury.

Now we will go to Chief Demkiw for five minutes, please.

Chief Myron Demkiw (Chief of Police, Toronto Police Service): Thank you, members of the Standing Committee on Public Safety and National Security, for the invitation to join you today.

The Toronto Police Service, along with the broader policing community in Canada, has long advocated for reforms that put public safety first, including reforms related to lawful access. We believe that Bill C-22, an act respecting lawful access, is a step in the right direction. It would provide additional tools for our officers to move investigations forward more quickly, hold offenders accountable and prevent harm.

Preventing harm often requires the ability to intervene early, including in cases involving violent extremism.

The Toronto Police Service is the biggest municipal police service in Canada. Policing in Toronto is extremely complex. In addition to all the unique aspects of the city, we often see trends here before they begin to appear in other areas. We see the ripple effects of geopolitics and a rise in hate crimes. We see frontline situations rooted in the complexity of mental health, addiction and unmet social needs.

Toronto is home to the majority of consular offices in Ontario. The city is host to many major international events. We are seeing more young people becoming involved in violence and often communicating anonymously about potential targets through digital platforms.

Addressing these issues requires support and collaboration across the broader justice system, including through legislative reform. In many ways, new technology and communication enhancements have made our lives easier, but they have also made it easier for criminals to plan their activities and avoid justice. We are seeing bad actors use digital tools for all kinds of crime, including drug trafficking, extortion, child pornography, hate crimes, extremism and other serious offences.

Our role is to prevent these offences, bring offenders to justice and provide a voice for victims who have experienced some of the most difficult of circumstances. However, because technology has evolved so quickly in recent years, we are encountering roadblocks in some of these investigations.

Take, for example, the issue of confirming which telecommunication service provider has information that will assist in an investigation. Presently, this process is time-consuming and potentially leads to loss of evidence. Bill C-22 would streamline our processes and allow police to advance investigations in a timely manner.

As the criminal world evolves, law enforcement and the justice system must keep pace. It is important to note that some of these tools are already available in other Five Eyes countries. The Toronto Police Service strongly believes that lawful access would reduce delays in accessing critical information and, in doing so, enhance public safety.

Thank you. We look forward to continuing our work with all levels of government to ensure the justice system upholds accountability and protects our communities.

● (1550)

The Vice-Chair (Frank Caputo): Thank you, Chief Demkiw.

With that, we will get to our first round of questions. I will exercise my prerogative as chair to take six minutes for questions. This is something that I've spoken about with the honourable parliamentary secretary and my colleague from the Bloc.

Thanks to all of you for being here. This is an area in which you all have a lot of expertise.

I thank the two police chiefs for their service.

Professor West, it will probably be no surprise that I'm going to start with you. I wanted to ask you about encryption. This seems to be, for some people, a really big issue.

What can you say about encryption when it comes to this bill? Is it sufficiently defined? Is it not sufficiently defined? Where, in your legal opinion, would you land, given what we see in the bill on the definition of "encryption"?

Leah West: As I read the bill, there is no means by which the government could say that you have to force open your encryption if you don't already have the capabilities.

I say that because, both for the regulations and for the ministerial orders, it says that you cannot comply with an order or regulation if it requires instituting a "systemic vulnerability" into your system, and the way that systemic vulnerability is currently defined includes encryption, because of the definition of "electronic protection".

My concern is more over the fact that there could be other forms of systemic vulnerabilities built into the hardware or operating system that don't get captured by the definition of "systemic vulnerability". That's where I see a gap.

The Vice-Chair (Frank Caputo): Okay. I'm going to have you expand on that, please.

When you talk about these vulnerabilities, I assume these might be vulnerabilities that the provider might not even know about. Is that accurate?

Leah West: That's correct. However, because we don't know who a core provider would be and who could be captured by this act, there could be hardware providers, for example, that could be service providers that would be captured, and the definition of "systemic vulnerability", as it stands, wouldn't capture their activities.

I know you're going to hear from Professor Diab later. He also has thought about this as well, so I would turn to him for more on that.

The Vice-Chair (Frank Caputo): Right, because in the legislation, part 2 would apply to those who meet the definition of a "core provider", or if I recall correctly, those who are designated by ministerial order. Is that—

Leah West: That's my understanding, yes.

The Vice-Chair (Frank Caputo): Theoretically, a business could be designated by ministerial order, and it would then be subject to this. Essentially, if I properly get what you're saying, that's boundless or limitless, in that we don't know exactly who this is going to be applied to. Do I have that right?

Leah West: My understanding is that they would still have to be an electronic service provider. However, the definition of "electronic service provider" is fairly broad, so it could capture people who provide hardware services, for example.

The Vice-Chair (Frank Caputo): I'm going to ask you about something, and this is an interesting question that was brought to my attention. Let's say that a business provider has a capability.... It's Alexa, for instance. That's Amazon, I believe. Is that right? It's something like that. Alexa, theoretically, could listen to your conversations, or every time you say, "Hey, Siri," Siri starts to listen.

Could it be possible that if Apple has the ability—I'm sorry to pick on Apple—or any company has that ability, they could say, "Okay, every time that someone says, 'Hey, Siri,' that app has to start listening"?

The app itself or the provider itself has the ability to listen. It's actually not necessarily asking the provider to create a new power. It's almost asking for it to go one step further.

Are you with me so far?

Leah West: Yes.

The Vice-Chair (Frank Caputo): As I understand it, if such an order were made, that order would not "possibly" be secret but would be secret, in which case a whistle-blower couldn't necessarily come forward. I guess the only recourse there for the company that's doing that would be to apply for judicial review. Is that accurate?

● (1555)

Leah West: If there were a ministerial order to have that capability, that ministerial order would have to be reviewed by the IC and approved, and then, yes...but with consultation. There's consultation built in to require that consultation—with Apple, in this case. If that approval were still done, then there would be JR.

However, you have to layer on top the fact that nobody could access that lawfully without a warrant for interception. Just because the service provider would have the capacity doesn't necessarily mean that law enforcement would then, all of a sudden, have access. In that case, you wouldn't really be instituting a new vulnerability because they already had the capacity. Really, you're just giving law enforcement the capacity to tap into something that already existed, if they had lawful authority.

The Vice-Chair (Frank Caputo): Right. I suppose that, in this case, the difference might be that the police could say, "We believe Professor West has committed a criminal offence, and that her use of Siri holds evidence of that. We are going to get a warrant." They could get that now. The only difference is that, under part 2, there would be a requirement to bring up the capacity to do that or the capability to do that, whereas right now it would just simply exist—if that makes sense.

Leah West: That's my understanding.

The Vice-Chair (Frank Caputo): Okay. Thank you.

My six minutes are up.

[*Translation*]

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

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

My question is for the two law enforcement representatives. One important thing to keep in mind here is that Bill C-22 aims to give law enforcement the means to act in a timely manner.

Chief Demkiw, you said that the process was time-consuming and that this could lead to the loss of evidence.

Also, in your opinion, in cases of online fraud, cybercrime, extortion and vehicle theft, am I correct in thinking that acting quickly helps reduce the number of victims?

If an investigation takes a year or 18 months, there could be hundreds of victims rather than just a few or a few dozen cases. In cases of cybercrime or sextortion, there can be many victims.

That's what I would like clarification on. There's a big difference between having one victim or 200, between having one case of cybercrime or 12.

This is where Bill C-22 needs to make a difference.

What are your thoughts on this?

[*English*]

Chief Myron Demkiw: The short answer is, yes, time is of the essence, and whenever time is of the essence, in cybercriminality, fraud or extortion, you certainly risk greater victimization, both in the number of victims and in the impact on individual victims. As we know, sometimes people are victimized many times over.

To your point, as our investigations are sometimes hampered and as it takes longer to unravel the digital evidence that needs to be uncovered to stop the victimization and criminality, more people are victimized.

Jacques Ramsay: Chief Fleury, would you like to add to this?

Chief Darcy Fleury: Yes.

Given the example of fraud-related offences that you used, let's take an example of a Ponzi scheme. In a Ponzi scheme situation, if we've identified one, two or three victims and we're able to get into that material or that information early on, there's a really strong possibility that our quick access to that information will stop further victimization or prevent other people from becoming victims before we finish up the investigation.

I have seen that happen in the past when time was of the essence. We're talking about people who are very motivated to do their crime, and they will victimize multiple people very quickly. If we have the ability to get in there, we might be able to interrupt some of their activity while we're forming grounds to lay charges and go forward with court proceedings. I think it's really important to have that early access in those types of scenarios.

● (1600)

[*Translation*]

Jacques Ramsay: Thank you.

We sometimes get the impression that some people would like to portray Bill C-22 as excessive. On the contrary, I believe that the government has shown a lot of restraint with this bill and focused solely on what is essential. At one point, there was a proposal to request information on taxis and on what happens at night in hotels. The government decided to limit those powers.

In your opinion, does Bill C-22 represent a well-considered piece of legislation that seeks only essential information?

[*English*]

Chief Myron Demkiw: If I may start, the short answer is, yes, I believe it is.

We know from practical experience that the use of digital technology by the criminal element has expanded dramatically, and our ability to gather timely evidence, preserve evidence and prevent the escalation of offences is hampered by the inability to access key digital bits of evidence. Bill C-22 will assist us in that regard.

By way of a simple example, when we have a phone number tied to a particular set of criminality, no matter how serious the alleged crime, we have to establish who the service provider is, and that in and of itself is a cumbersome task today. Bill C-22 will streamline that task, allowing us to move more quickly and gather essential evidence that may disappear and be lost while we wait for different service providers to advance our investigations under the current legislative framework.

Bill C-22 is calibrated well to assist us in making timely access to key digital technology more readily possible.

Chief Darcy Fleury: Yes, I agree with Chief Demkiw. I think it's very well put together and addresses those areas where data moves so quickly. It does a good job of collecting that.

Jacques Ramsay: Ms. West, I believe Canada and Australia are the only countries where there is explicit prohibition against, for electronic protection safeguards, implementing a capability that would introduce a systemic vulnerability. For instance, in the U.S.A.—

[*Translation*]

The Vice-Chair (Frank Caputo): I'm sorry, Mr. Ramsay. Your time is up.

[*English*]

No, I didn't look forward to saying that.

[*Translation*]

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

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

Dr. West, in a joint letter, several civil society organizations have expressed concerns about Bill C-22. They say it could facilitate increased information sharing with foreign governments, including countries with human rights practices that are of concern.

What additional safeguards should be considered to limit the subsequent use of Canadians' personal information?

[*English*]

Leah West: I think there are two issues.

The first is on changes to the MLAT, which would allow foreign entities to serve orders in Canada. There would be a process where the minister approves the request, it goes through a judge, the judge agrees that the criteria made out in the Criminal Code are met, and then they collect that data back.

There is no requirement that the law under investigation also be a crime in Canada, so there is the possibility of seeing foreign governments seeking to enforce repressive laws or politically motivated investigations through this process. There is no real safeguard against that, except for the actions of the minister executing things at his discretion. In this case, especially because there isn't necessarily a judge involved in the foreign jurisdiction, it can be an administrative order. The minister has to commit to exercising his discretion to not authorize a process where the crimes being investigated are potentially repressive or politically motivated. There is no safeguard in the law.

There could be by adding the fact that the law would similarly have to be a crime in Canada. Then we wouldn't have that problem. That's one way to make it broader. However, right now, it would be at the minister's discretion.

● (1605)

[*Translation*]

Claude DeBellefeuille: Thank you.

I'm very concerned about this. So if you could suggest a specific amendment to Bill C-22 that might reassure people, that would be very helpful. We have until May 27 to introduce amendments.

I'd like to ask you another question. In the letter you published in The Globe and Mail, you emphasize the importance of the work being done in committee and of reaching a consensus around Bill C-22. I think everyone here would agree that this bill is necessary, but that it could be improved.

Do you think it would be reasonable to include the National Security and Intelligence Review Agency, so that it is notified in real time when a ministerial order is issued, and so that it can investigate and ensure that the powers conferred by Bill C-22 are not abused?

[*English*]

Leah West: No, I don't think so. The National Security and Intelligence Review Agency is a review body. It engages in *ex post facto* review. It doesn't have a current mandate to engage in oversight.

I personally recommended that the intelligence commissioner be involved in reviewing ministerial orders, because they have that role of oversight in the current system and they are set up to do that in a way NSIRA is not.

[*Translation*]

Claude DeBellefeuille: Okay.

The idea is not for the National Security and Intelligence Review Agency to participate in the decision or give its opinion on the continuation of the ministerial order. Rather, it's a matter of ensuring that the agency is notified in real time so that it can document a case that, once a year has passed, might be easier to handle should an investigation ever be launched.

Thank you for clarifying your opinion because, even with the help of interpretation, it's a bit difficult for me to understand.

[*English*]

Leah West: I certainly see a role for NSIRA in reviewing the system in general and potentially a role for your colleagues on NSICOP down the road. That will be exceptionally important, particularly in looking at how the role of engagement with the service provider community is rolled out.

Whether or not NSIRA needs to be informed every time there's a ministerial order in order to do that.... Again, I think it's more set up for a longer-term review. It would be best receiving information at the end of the calendar year or every six months. I don't really think it's in a position to do case-by-case reviews.

[*Translation*]

Claude DeBellefeuille: You said that the definition of “electronic service provider” is very broad and that it could include hardware providers, for example.

Could you give us some examples of hardware providers?

[*English*]

Leah West: Typically, anyone who provides hardware often also provides some sort of electronic service. I think hardware providers, like Ericsson and others that operate in the hardware space, could find themselves captured by the broad definition.

I don't think that's necessarily wrong. I think the definition—

The Vice-Chair (Frank Caputo): I'm sorry, Professor. We'll have to pick that up in the next round.

We will move on to Ms. Kirkland for five minutes, please.

Rhonda Kirkland (Oshawa, CPC): Thank you.

My questions will be for Ms. West.

I appreciate your testimony here.

Given that this is our ninth time, as you said, trying to get this legislation right in terms of lawful access, how important is it—you talked about striking the right balance—that we're not racing to royal assent and that we are taking the time to review amendments and listen to testimony?

● (1610)

Leah West: In my opinion, it's crucial to getting the bill right.

Rhonda Kirkland: Thank you.

You have said publicly that the government should show its homework. I appreciated that, especially the focus on this committee, which is part of making this legislation go through this process.

We know that in consultation with Murray Rankin, who produced a report that informed Bill C-22.... The Minister of Public Safety told the committee that the report was used specifically to inform the government's decision-making on Bill C-22. I know you participated directly in that consultation.

In your professional opinion, is there any legitimate national security solicitor-client privilege or operational reason preventing the report from being released to Parliament or to the Canadian public?

Leah West: I'm not privy to the relationship that Murray Rankin had with the minister when he offered his advice, so, no.

Rhonda Kirkland: From your perspective as a participant in the process, how central was the consultation exercise to shaping the lawful access now before Parliament?

Leah West: In my opinion, it reflects the type of advice I was hearing as part of the consultation process.

Rhonda Kirkland: To your knowledge, were participants in the consultation process ever advised that the report or its findings would remain confidential from Parliament?

Leah West: That wasn't something that was discussed.

Rhonda Kirkland: You never discussed that. Okay. Thank you.

I have just one more question.

In your experience, is it typical? You've probably been part of these processes before. I assume you have been; I could be wrong. Is it typical for consultation reports involving external experts and stakeholders to be withheld entirely? Have you seen that before?

Leah West: I've never been involved before in a consultation that was run by an external party, so I'm not sure. Typically, I've been involved in consultations that are run by the government itself, and they usually—

The Vice-Chair (Frank Caputo): I'll interrupt for just one moment, please.

We have a meeting here. I don't mind whispers; I know that's going to happen. If it needs a meeting, we should go outside, please. Thank you.

I'm sorry about that.

Leah West: That's all right.

I've never been involved in a process similar to this. In the past, in government consultations, I've seen “what we heard” reports be published. This was a different kind of process.

Rhonda Kirkland: It sounds like, in part of the process, you may have seen the report. Can you comment on whether it would be helpful for us in...?

Leah West: I didn't see the report.

Rhonda Kirkland: Okay.

Leah West: I saw a list of recommendations.

Rhonda Kirkland: You saw a list of recommendations.

Without disclosing anything confidential that you may have seen, can you tell the committee if the report reflected a diversity of views? Do you know if there were recommendations including concerns and cautions raised by experts and stakeholders in terms of privacy?

Leah West: Yes, because my own concerns were reflected in the list of recommendations.

Rhonda Kirkland: Thank you.

Beyond that report, I would like you to expand the specific recommendations you have for amendments. Could you give one or two that you think would really make this bill a much better bill? We know about lawful access and how important it is. I appreciate the chiefs in the meeting today because of how important it is.

Can you give us one or two amendments that could seem fairly simple and that you think we could all agree on in order to get this right versus racing...?

Leah West: Yes.

As I mentioned, I would implore the committee to hear from technical experts who know, better than a lawyer, how to capture all the types of vulnerabilities you would like to avoid in the definition of “systemic vulnerability”. I also think that the current retention provision as drafted is overbroad. We've seen similar provisions, even more narrowly tailored ones in Europe, to be found to engage the right to privacy and be unreasonable. I think that provision in and of itself needs to be reformed to ensure that any regulation is narrowly targeted, necessary, proportionate and reflects the seriousness of what they're asking for, which is the creation of large pools of private data.

Rhonda Kirkland: Thank you.

We know that broad definitions often lead to future governments misusing or abusing legislation—

The Vice-Chair (Frank Caputo): Unfortunately, Ms. Kirkland, your time is up.

Up next is Ms. Acan for five minutes.

● (1615)

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

Dr. Leah, it's great to see you again.

My question for you will be on foreign entity requests. Canada is currently the only Five Eyes and G7 member without modernized lawful access legislation. Does our lack of a technical capability framework hinder our ability to co-operate with international partners on transnational threats? How does part 1's new mechanism for foreign entity requests solve this problem?

Leah West: Yes, it does.

Talking to folks across the Five Eyes, my understanding is that in other jurisdictions the threshold upon which they can obtain subscriber information is lower than that in Canada. Often it's not required to be judicially authorized, or it might be on a reasonable suspicion standard or even lower than that. When they try to use the MLAT process in Canada, there's no parallel in Canada that would allow us to enforce their orders.

Having a new provision focused specifically on subscriber information and transmission data with a threshold of reasonable grounds to suspect would allow us to partner better with foreign jurisdictions because it would be more in line with how they obtain subscriber information in their jurisdictions and allow for equitable enforcement.

Sima Acan: Thank you very much.

I'll focus primarily on the operational side of policing and ways to support the work that the investigators do when it comes to organized crime, extremism, child sexual exploitation and other complex crimes.

Chiefs, Bill C-22 creates a confirmation of service demand, which simplifies the process by which law enforcement identifies the proper recipient of a production order. Would you say that this helps in the context of a time-sensitive investigation dealing with organized crime, extremism, hate or child exploitation? How does this provide the main operational benefits to you?

Chief Myron Demkiw: Thank you for that.

I think the practical reality is that we often have a phone number or another clue that requires us to then pursue the digital footprint, the digital evidence, that the phone number or other information provides.

In the present regime, there is no provision for us to make a demand for service providers. We have to do production orders multiple times to simply identify that this is a service provided by a particular telco, for example. There's an incredible amount of time spent doing this. Just by way of example, numbers-wise, over a 20-month period, our detective operations alone in Toronto did 1,900 production orders.

Something that would help us very much is to have the ability to understand which service provider to focus our investigative efforts on and to then pursue that through a judicially reviewed process: production orders or warrants. That saving of time is very real and will impact our ability to succeed.

As was asked in the previous question, the type of evidence that can get lost while we determine who the service provider may be—video evidence, forensic evidence—may involve greater victimization or ongoing victimization that proceeds for a longer period of time while we, in the present regime, determine who the service providers are. The ability to know where to focus our investigative energy quickly and then to go through the process of gathering evidence through production orders, which are scrutinized by a justice, is something that we very much welcome.

Sima Acan: Thank you very much.

In this context, Bill C-22 has metadata retention requirements where metadata is to be held for up to 12 months. Yesterday, we heard from officials that in Australia they keep it for two years. In the U.K., they keep it for one year.

Would you say that requiring core providers to retain metadata for 12 months is a reasonable time frame, given the fact of how quickly providers may otherwise delete the data? Sometimes it's 30 days. Sometimes it's three months.

This is still remaining flexible for providers and supportive of investigators, especially when complex cases can go beyond three to six months or even over a year.

Chief Darcy Fleury: Maybe I will start with this one, and the chief can follow up.

Yes, I think 12 months is a good start, but yes, obviously you're right. If the investigations are prolonged, and they can be very long in some of these cases, retention beyond the 12 months—24 months or 36 months—would be ideal.

● (1620)

The Vice-Chair (Frank Caputo): I'm sorry, Chief Fleury. We have to cut you off there.

[*Translation*]

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

Claude DeBellefeuille: Thank you, Mr. Chair.

Dr. West, you heard the two police officers discussing data retention periods. You told us that one year is too long. The people who work for police services have just told us that, for them, one year is the minimum and that two or three years would be even better.

How do you see things?

Do you lean more toward a shorter retention period? How do you respond to what the other witnesses just said?

[*English*]

Leah West: I certainly understand from the law enforcement perspective why they would want all the data they need to be available for as long as necessary, but in terms of charter protections, my opinion is informed by what I've read of European jurisprudence on this issue.

Also, it's not just that it's one year. It's one year for any type of data for any purpose: for mischief or for investigating jaywalking, for example. I'm not saying that's what they would do, but it's the fact that it's for any purpose, for any type of data, that creates a chill in people that they could be under surveillance when all of their data is being held for this long period of time.

Right now, there's nothing that constrains the retention. It's any type of data for a year, for any purpose, and I think that's what needs to be amended to make sure that it's more narrowly tailored to the type of data, the requirement and the investigative imperative.

[*Translation*]

Claude DeBellefeuille: If we want to share information with the Five Eyes, shouldn't we retain metadata for the same period, on average, as the countries we collaborate with?

[*English*]

Leah West: In the Five Eyes, it's varied. For example, in Europe and the United Kingdom, it's only for serious crime, so it's not for everything that they can go and retain information for a year. In the United States, their authorities don't allow for year-long retention; that's not part of their act. Every—

[*Translation*]

The Vice-Chair (Frank Caputo): Mrs. DeBellefeuille, your time is unfortunately up.

[*English*]

Mr. Lloyd, you have five minutes.

Dane Lloyd (Parkland, CPC): Thank you.

Thank you to the witnesses for being here.

Dr. West, one concern I've heard is that many tech companies advertise that they have privacy controls. For example, companies that have smart devices in homes advertise that the microphones can't be turned on remotely so that they can listen. Under this legislation, it's kind of odd to me that it talks about how it's not here to look at content, but ministerial orders can order these companies to provide the capabilities to turn a remote microphone on. Is that correct?

Leah West: When they talk about content, that's in terms of retention of data. It does allow for the creation or ordering of intercept capability, so that would be an intercept capability. You could potentially have an order that would require that capability and as long as it didn't create a systemic vulnerability, yes, it could be implemented and they would have to change their advertising.

Dane Lloyd: Now, that creates a bit of a conundrum, because what if it's a secret ministerial order?

Leah West: True. I don't have an answer for you.

Dane Lloyd: For the benefit of the committee and those watching, if a company says that remote microphones can't be turned on and the government issues a ministerial order saying you need to build in the capability to turn on a remote microphone, the company in question could not change its advertising to say it would not turn on your microphone without violating the very non-disclosure and secrecy clause. They would still be advertising that they would not turn on remote microphones while the government has forced them to create that capability for law enforcement.

● (1625)

Leah West: I'm not sure how a company would manage that situation.

Dane Lloyd: It's just an issue for me, I think.

On another aspect, I'm concerned about this blanket metadata you've talked about. I can certainly understand that if you suspect that somebody or a group is involved in criminal activity, you could order.... I think that already exists; preservation orders already exist. However, if we're talking about a blanket requirement that the metadata of all Canadians and all people residing in Canada be kept for up to a year, that creates a lot of very interesting constitutional privacy law.... Do you have any thoughts on that?

Leah West: I agree.

I listened to the questioning in the last testimony about whether or not this creates a seizure, and if it doesn't create a seizure would it still violate section 8. I think there would be a serious chilling effect and a belief that people lacked privacy because, ultimately, the state could then get access through a transmission production order or a tracking production order, or even location data, for any crime going back up to a year. That does create a chilling impact and would have serious implications for how people viewed their right to privacy in Canada—and it wouldn't just be people in Canada. It would be anyone who has services with a Canadian company.

Dane Lloyd: I'm less concerned about the people committing crimes. I'm concerned about the innocent Canadians whose metadata is going to be collected. Are you at all concerned...?

We saw the Salt Typhoon hack in the United States, where some very sensitive personal data was hacked by foreign agents. It was discovered after the fact that it was the systemic vulnerabilities that were required by the U.S. government that allowed for this. I know the legislation says that it doesn't want to create systemic vulnerabilities, but I'm not sure that lawful access can be facilitated without creating.... You said there's a risk. Then we're also talking about forcing companies to keep people's metadata—blanket—for the whole country for an entire year.

Are we not creating a treasure trove of people's personal data that hackers are going to want to have access to?

Leah West: As I said in my opening statement, any point of access created that didn't previously exist and any pool of data you're creating that didn't previously exist create new risks, so the regulatory framework—

The Vice-Chair (Frank Caputo): I'm sorry. I have to cut you off, Professor West.

[*Translation*]

It's hard to stay within the time limit when we get to the last questions.

[*English*]

It's tough but fair.

With the final questions, we have Dr. Powlowski.

[*Translation*]

Marcus Powlowski (Thunder Bay—Rainy River, Lib.): Do I need to ask my question in French?

Voices: Oh, oh!

Marcus Powlowski: I'm told it's not necessary.

[*English*]

Darcy, it's good to see you out there, even though you're on a screen. I've gotten to know Darcy pretty well over the last few years. I have to say he's a wonderful chief in Thunder Bay. I'm really glad you're here.

You gave one concrete example of a 14-year-old girl. Maybe you can tell me, after I finish posing this rather lengthy question, whether that was a real case. I wonder about other cases you've encountered—you may want to disguise sufficiently whom you're talking about—where lawful access would have been helpful to you. I would think in terms of child pornography....

Especially in a place like Thunder Bay, there seems to be a real issue with trafficking people. There's also, as we both know, a big issue with gangs from Toronto and Ottawa coming up to Canada...well, not Canada. I guess it's Canada down here in Toronto and Ottawa as well. They're coming up to Thunder Bay and committing crimes there. There must be communications between the gangs going back and forth between Toronto, for example, and Thunder Bay.

Can you give other examples of how lawful access would help you in doing your job and addressing these problems?

Chief Darcy Fleury: The real case is of those youth who are coming up to us from down south. We see them on a regular basis. Some are as young as 14 years old. Of course, we have concerned parents who are reaching out and asking for some support. They go originally to the Toronto police and then come to us. They're asking for some support to locate these kids.

Really, when we're talking about the exploitation of these youth, they're getting involved in all kinds of different crimes and gang activities. Having in the legislation more immediate access would be a real benefit to us. When we start to see the chains and the links between some of the groups down south and these kids who are coming up here, it would be really beneficial to us to get ahead of it, especially when we're looking for these youth. We have real-life cases of families who have come up and asked us to go out and help search for their youth. Quite often, we find them involved in drug activities or the gang-related work that's being done in this community.

That happens on a regular basis. On average right now, I'd say we've probably gone from 60% to 50% of the people involved in that type of activity coming from southern Ontario. Again, they are very young people who are involved and exploited. We are looking at some of those cases. Are they being human-trafficked? They are coming into our flophouses, and then they end up doing all kinds of activities.

This is a real concern for us. I think if we had the ability to access a bit sooner, it would be a definite benefit to us to enforce some of the acts that we do.

● (1630)

Marcus Powlowski: Chief, I could see in that situation, where young people aged 15 or 16 are coming up and getting involved in crimes, how you might want to be able to access their data, for example, on their cellphones, on their Internet or in their emails. That's desirable, but there's a concern about the slippery slope. Although that may be desirable, how do I know this doesn't involve looking in on...?

I have a 17-year-old boy. He has his social circle. They have girlfriends. They're always socializing back and forth. How do I know that basically everything they do, including talking to Siri, doesn't go to the police? That would seem to be an unnecessary violation of things we think ought to be confidential.

Chief Darcy Fleury: That's right. I think police services across the country are very good at identifying the specifics of what they're looking for. Going back to my presentation, this is not about an overarching, wide open playing field for police to go into and get what information they want. It has to be specific to the event we're looking for.

For example, if we have a missing youth from southern Ontario, we would investigate that as a missing youth. If we had access to their data and the material they had, it might show those connections immediately that would allow us to start formulating a bigger investigation, along with the contacts and associates they have who may be in Thunder Bay or down in southern Ontario. It would really help us further our investigation a lot quicker and perhaps resolve some of the victimization or even some of the illegal activity they might be doing.

It would be very focused. It would not be wide open.

Marcus Powlowski: Ms. West, could I ask you a question?

I hadn't thought about something like Siri, but that's Internet data. If my 16-year-old kid asks me something and I jokingly say, “Well, if you do, I'll beat you with a baseball bat,” and Siri picks that up—

The Vice-Chair (Frank Caputo): Unfortunately, Dr. Powlowski, that is the last thought of this round.

Some hon. members: Oh, oh!

The Vice-Chair (Frank Caputo): I'd like to thank all of our witnesses for being here.

Anthony Housefather (Mount Royal, Lib.): It was just getting good.

The Vice-Chair (Frank Caputo): We will suspend to bring the next witnesses on board.

● (1630)

_____(Pause)_____

● (1635)

The Vice-Chair (Frank Caputo): Thank you, all, for being here again for the second hour.

We have two witnesses here in person and one appearing by video conference. I understand that Mr. Fraser, who is on video, has been sound checked.

Thank you for appearing.

We also have Dr. Robert Diab from Thompson Rivers University.

Lastly, we have Dr. Michael Geist from the University of Ottawa.

Professor Diab, could you please go ahead with your five-minute opening statement?

Robert Diab (Professor, Faculty of Law, Thompson Rivers University, As an Individual): Thank you, Mr. Chair and members of the committee, for the invitation to appear today.

I'm a professor in the faculty of law at Thompson Rivers University, and my area of specialty is section 8 of the charter, which protects against "unreasonable search or seizure".

I want to begin by acknowledging that Bill C-22 marks a meaningful improvement over its predecessor, Bill C-2. Several of the powers in the bill have been more appropriately tailored—

The Vice-Chair (Frank Caputo): Wait one moment, please, Professor Diab.

I understand we're having some difficulties.

Anthony Housefather: I'm just wondering if Professor Diab might be able to speak up, because I'm having trouble hearing him.

● (1640)

Robert Diab: Okay, thank you. I'll try.

Anthony Housefather: Thank you, Mr. Chair.

The Vice-Chair (Frank Caputo): Thank you.

Robert Diab: Several of the powers in the bill have been more appropriately tailored to the needs of law enforcement and to the privacy interests at stake, but I would like to highlight and briefly walk the committee through what I believe are three significant weaknesses with the bill that remain.

The first is the new production orders for subscriber information to be added to the Criminal Code. The government's charter statement defends this power on the basis that subscriber info is not particularly sensitive, since it reveals only the name and address of a person obtaining a service from an entity like Rogers, but the power as drafted would disclose much more than this. Police can obtain not only a name and address tied to an account, but also the types of services a person subscribes to, the tiers or channels associated with those services and the identifiers of every device associated with the account.

It also applies to any person who provides a service, not just companies like Rogers. All of this certainly allows for capturing sensitive information like, for example, what cable packages a person subscribes to or what medical services they receive. A power to obtain this shouldn't rest on reasonable suspicion alone. The scope of the power should be narrowed. As it stands, I think it would likely be struck down under section 8.

A second concern I would like to raise is the definition of "systemic vulnerability". I understand that Professor West dealt with this earlier, but I'll try to target my remarks here. There is a definition, and that's good, but it remains too narrow in two ways.

The test for what constitutes a vulnerability here is defined to be one "that creates a substantial risk that secure information could be accessed by a person" without authorization. That's too high a threshold. Developments with AI in recent weeks reveal its far greater power for hacking, so even a remote or theoretical vulnerability now could be readily exploited.

The definition also applies only to vulnerabilities in the electronic protections of an electronic service. It may not extend the definition to the operating systems of devices, so a ministerial order could, in principle, require Apple or Google to build extraction capabilities into an operating system without engaging the safeguard, even if the practical effect would be to undermine end-to-end encryption.

The third concern with the bill is, in my view, the most serious, which is the metadata preservation power that the committee spent time on a few minutes ago. This would require core providers to retain transmission data for every communication for up to a year. That's when and where we used our phones and the coordinates of who we were in touch with, when and where.

The charter statement doesn't address this at all. Its position appears to be that compelling a provider to preserve metadata is not itself an interference with privacy, because police still need a warrant or other authority to access the data. It implies that it is not a seizure and does not engage section 8, but this is not so.

We know from ample case law that metadata is private, and under these provisions, when the minister compels Shaw or Telus to preserve our metadata, the company is doing so on behalf of the state and for a law enforcement purpose. Those are the basic elements of a seizure under section 8.

It's worth noting that Parliament assumed precisely this 12 years ago when it added to the Criminal Code the power to make a preservation demand or order, which requires individualized suspicion, reasonable suspicion or a warrant, depending on the case. This is key: It makes it a criminal offence to hold data, if you're Shaw or Telus, etc., beyond whatever the period at issue is. Why would Parliament have assumed authority was needed to preserve data if it didn't engage section 8?

Nothing here changes, in my view, in light of the fact that police are saying they won't look at it unless they go get a warrant. That's also true right now. In order to see the things they demand to be preserved, they need a warrant, but even preserving it is—

The Vice-Chair (Frank Caputo): Thank you, Professor Diab.

In Parliament, we're used to it going down, so I apologize for cutting you off.

I would like to welcome MPs Kayabaga and Baber to the table as well.

Dr. Geist, please go ahead with your five-minute opening statement.

● (1645)

Michael Geist (Canada Research Chair in Internet and E-Commerce Law, Professor of Law, Faculty of Law, University of Ottawa, As an Individual): Good afternoon, everyone. Thank you for the invitation.

My name, as you heard, is Michael Geist. I'm a law professor at the University of Ottawa, where I hold the Canada research chair in Internet and e-commerce law. I appear in a personal capacity, representing only my own views.

In preparation for today's hearing, I looked back at the history of my engagement with lawful access policy. I found that I wrote my first op-ed on the issue more than 20 years ago, and first began appearing before committees, about various bills, a few years after that.

As I'm sure you know, lawful access has been the subject of legislative debate in Canada for decades, under both Liberal and Conservative governments. The technologies change and the governments may change, but the challenge has always been the same: to give law enforcement and security agencies the tools they need to address serious crime while respecting Canadians' privacy rights and the constitutional framework the Supreme Court has built around privacy in decisions such as Spencer and Bykovets.

Bill C-2 is what happens when the balance is not well struck, as its warrantless information demand power envisioned compelling disclosure of subscriber information, of any provider of a service in Canada, without court oversight. The decision to drop that power was the right one, and replacing it with a confirmation of service demand is a meaningful change. Bill C-22, nevertheless, contains some serious problems, and I'll focus on three. They're going to echo what we just heard from Professor Diab.

First, I'm going to focus on the mandatory metadata retention regime, which would require providers to retain metadata for up to a year on every subscriber, regardless of suspicion. On a mobile network, that data includes cell towers each phone connects to. When retained at scale, the aggregate amounts to a comprehensive surveillance map of virtually every Canadian, where and when they go, and who they interact with. This is the kind of bulk data retention regime that the Court of Justice of the European Union struck down in the Digital Rights Ireland case, and in the Tele2 Sverige case extended to mandated private sector retention of traffic and location data. Germany's Federal Constitutional Court has reached similar conclusions, yet, remarkably, the charter statement about Bill C-22 fails to address the regime, despite the obvious charter implications.

The committee is being asked to entrench a surveillance architecture and accept the security risks that come with it. The obvious approach is to remove this entirely, as it is disproportionate and, I believe, likely to be struck down in its current form by the Supreme Court. Alternatively, perhaps a 30-day cap on metadata retention would suffice in terms of meeting the immediate investigative needs, while allowing for a court order if a longer period is required.

The second concern involves systemic vulnerability safeguards in the technical capability provisions. Proposed sections 5 and 7 of the SAAIA—that's part 2—say providers are not required to comply with an order if doing so would create a “systemic vulnerability”. Proposed sections 12 and 13 make compliance unconditional and provide that orders prevail over inconsistent regulations. That leaves a safeguard that exists in name only, largely cloaked in secrecy, with the burden of invoking it falling on the providers. The consequence is a backdoor capability mandate that could weaken encryption, place user data at risk and lead companies to remove privacy-enhancing services from Canada.

This needs a fix, which should include amending proposed section 12 to make compliance subject to the provisions of proposed sections 5 and 7. Further, the definition of “systemic vulnerability” should be expanded by the statute, clarifying that there will be no requirement to weaken or break encryption or to introduce any security weakness.

The third concern is the production order threshold for subscriber information. Bill C-22 sets the standard at “reasonable grounds to suspect” rather than the current “reasonable grounds to believe”. The Spencer and Bykovets decisions establish a high informational privacy interest in subscriber data, yet the charter statement nevertheless asserts that the “subscriber information sought does not, by itself, constitute particularly sensitive information”. I think that sentence is difficult to reconcile, both with Supreme Court jurisprudence and the technical reality of what subscriber information may reveal. Setting the bar lower invites further charter litigation, placing the provision on shaky legal ground.

Now, none of the changes that I've discussed here would be incompatible with effective law enforcement tools. Rather, they're about ensuring a framework that can withstand charter scrutiny, respect Canadians' privacy rights, avoid creating a surveillance infrastructure and sustain public interest and confidence.

● (1650)

I look forward to your questions.

The Vice-Chair (Frank Caputo): Thank you, Dr. Geist.

Now we move to Mr. Fraser for five minutes.

David Fraser (Partner, McInnes Cooper, As an Individual): Mr. Chairman and honourable members, thank you very much for the kind invitation to share my views on Bill C-22.

I'm a partner at the law firm McInnes Cooper in Halifax, where, among other things, I advise clients who are on the receiving end of orders for customer information. I also teach at the Dalhousie law school. I'm appearing in my personal capacity with my own views, and I'm not speaking on behalf of any of my clients.

I have to commend the government for its comprehensive consultation with stakeholders since Bill C-2, to which I contributed, but I still have a number of concerns and recommendations. I'll note that, in particular, part 2 of Bill C-22 is very problematic. I can't cover all my concerns in five minutes, so I look forward to the rest of our discussion.

First, I agree with my colleagues. We need to narrow the scope of subscriber information production orders or raise the bar up to reasonable belief. The bill lowers the threshold for police to obtain a production order for subscriber information—which they can get today—from “reasonable grounds to believe” to merely “reasonable grounds to suspect”.

The organizations that could be on the receiving end of these orders are any that provide services to the public, which include banks, hospitals, grocery stores and hotels. We're well beyond telcos here. Even though the definition is narrowed from ones in previous bills, police could still demand all the subscriber information that a service provider holds. This would go beyond name and address, as my colleagues pointed out. It would include the types of services provided and device identifiers, like the serial number of the CPAP machine from your doctor's office. It would compel Apple to hand over the digital IDs of every single device you have, including your AirTags and iPads. That's too much. I suggest narrowing the scope of these orders or raising the bar to reasonable belief. Otherwise, it will ultimately be found to have violated the charter.

I'll move on to part 2, the supporting authorized access to information act.

Nobody has made a compelling case for anything in part 2. The government has had 20-plus years to build its case, but, as NSICOP observed, it has only anecdotes. We should not be undermining the privacy and safety of every single Canadian based on anecdotes.

Part 2 of the bill targets electronic service providers, but the definition is so broad that it would likely include most businesses in Canada. Everybody deals with digital information. If it proceeds, the bill should include necessary guardrails. Under no circumstances should the government be allowed to require—particularly with a secret order—an electronic service provider to make changes to products or services it provides in the ordinary course, to collect and retain any data beyond what the business requires for its own purposes or to make any changes that would affect functionality, including adding additional functionality for any products or services offered by the business. As the bill is written, the Minister of Public Safety could issue a secret order to turn your Amazon Alexa into a listening device, as in an example given by the previous panel. CSIS has explicitly said, in connection with this bill, that it wants to be able to track every single cell phone in Canada in real time, and that telcos would have to change their services to make every cell phone trackable. That would be disproportionate and, in my view, absurd.

Now, the government says that it doesn't plan to undermine encryption and that there would be no back doors, but you just have to read the words in the bill to see that there's nothing to prevent this. Government officials said at this committee—I think it was on Tuesday—that the bill is “encryption-neutral”, but Canadians are not encryption-neutral. The words of the bill would clearly permit, and certainly would not prohibit, back doors and mandatory decryption. That would be in secret, with no transparency to Canadians and with very little accountability. What the government intends is not relevant. What is relevant is what words end up in the statutes.

Under part 2, the Minister of Public Safety could issue these secret orders to electronic service providers—very broadly defined—that come with mandatory permanent secrecy. Currently, the police and CSIS can apply to a judge for something called an assistance order. This orders a service provider to provide all reasonable assistance to give effect to a judicial warrant. It can be accompanied by a gag order if it's appropriate. That is judicial control. Nobody from law enforcement has offered evidence that assistance orders are inadequate or should be replaced by these secret ministerial orders. The U.K. equivalent of a ministerial order was used by the U.K. government to secretly order Apple to remove encryption on iCloud, globally. Part 2 of Bill C-22 does not contain any guardrails that would prevent such overreach in Canada. Secret ministerial orders have to go.

We also have the issue of metadata retention, which my colleagues already spoke about. This would include your location history. The government could require everyone's cell phone to become a retrospective tracking device going back a full year, without any suspicion of wrongdoing. This will almost certainly be found to have violated the charter. Collected metadata would be sought by Canadian and non-Canadian authorities based on mere suspicion. That would be a record of everyone who sought reproductive health care in Canada, which might be of interest to law enforcement in a Five Eyes partner.

● (1655)

Finally, as legions of cybersecurity experts—

The Vice-Chair (Frank Caputo): I'm sorry, Mr. Fraser. We will have to stop there. I apologize.

David Fraser: Thank you.

The Vice-Chair (Frank Caputo): As chair, I will be leading off this round for six minutes.

I want to thank all of the witnesses. We have a very academic panel this time. I'm very humbled by the three of you coming to spend your time with us today, and what do you know? We're all lawyers here. That's wonderful.

Professor Diab, it's particularly great to have you here as a colleague with whom I dealt at the bar in British Columbia in my time as a prosecutor and also in my time teaching advanced criminal law and sentencing at Thompson Rivers University. I know that everybody's very proud to have you here, so thank you for being here.

With that, I want to expand a little on the question of engagement in section 8 when it comes to the requirement of a third party to retain data. Is there a specific case you're relying on there, Professor?

Robert Diab: No, I'm just relying on the broad propositions under section 8. Section 8 is engaged whenever a state actor interferes with something over which we have a reasonable privacy interest, so I gather that the question you're asking is about a mere demand by a state agent of a third party to hold on to the private data that belongs to the person over there. Is that an interference with their privacy? Again, 12 years ago, Parliament assumed that, if a court were to look at that, they would find that it would be an interference with their privacy.

In other words, I can't think of a body of case law where police told third parties to preserve data and then it was challenged in courts. I can't think of that. The story for me begins with the power, the preservation power, and when that was added to the code, it was added, I'm assuming, on the premise that requiring a third party to do this for the state for a law enforcement purpose is an interference that engages section 8.

Once again, stand back and ask yourself how you would feel if you were told that Telus, Rogers, etc. are preserving a record of all your movements and the people to whom you sent emails, not the content but those details? How would you feel? They're preserving it for up to a year for the purpose of potentially prosecuting you if necessary.

Maybe one answer is that it's absolutely fine, but I think most Canadians and, I think, courts are likely to say no. They would think that the mere fact that I was visiting this person on this day or talked to this person is private. That should be private. There should be no record kept of it, and that is, I think, the best explanation I can give you as to why.

The Vice-Chair (Frank Caputo): Thank you.

I would like to ask the two professors who are here in person about the reasonable grounds to suspect versus reasonable grounds to believe. It's been a while since I dealt with reasonable grounds to suspect, but my recollection of reasonable grounds to believe is that there has to be a subjective belief, as in you have to personally believe that an offence has been committed, and that belief must be objectively reasonable. That's my recollection. In other words, a reasonable person would say, “Yes, you have a reasonable belief.”

It's below balance of probabilities, so it's not ultrahigh. It's less than 50%, but above the suspect, which is more than a hunch but less than that.

What would you say to the proposition that this is asking for very narrow data and, therefore, we don't have to worry as much that this could be saved under section 1?

Would you agree with that, Professor Geist?

Michael Geist: No, I wouldn't, and I wouldn't in two respects.

First, the consistent claim that this data is of low privacy value, I think, is simply inaccurate. We just heard examples from Professor Diab and, perhaps, over the course of the next little bit, we'll have a chance to walk through some of those kinds of examples, but it seems to me that, even with the question that came up towards the very end of your last panel about whether or not someone might know that you asked Siri something, the question isn't the content. The fact is that you raised it and engaged with people. The fact is that members of the public engage with you, and a record would exist of who you communicate with. The fact that there might be orders to have that kind of thing disclosed raises, from my perspective, significant issues.

This may have significant privacy import, so lowering the standard for this information, when there is scant evidence that the higher standard that we've had in place for many years now has posed a problem, seems to me unwarranted.

● (1700)

The Vice-Chair (Frank Caputo): I see.

To Mr. Fraser online, I mentioned at the last meeting, when I wasn't the chair, that this is a highly technical bill. We had only one hour with the officials.

I wanted to address one thing you brought up to this committee. You talked about CSIS wanting to have real-time access. I think the committee may want to ask CSIS about that.

For our reference and for our analysts, can you tell us where you got that point, please, in 25 seconds or less?

David Fraser: Absolutely. It was mentioned during the technical briefing when the bill was tabled. It was mentioned for Bill C-2 and again for Bill C-22. I have a copy of the slide deck that includes the illustration, if you'd like it.

The Vice-Chair (Frank Caputo): I'm sure we have that.

I have 10 seconds left, but we are a bit behind schedule, so we will now go to Mr. Housefather.

Thank you.

Anthony Housefather: Thank you, Mr. Chair. Ceding those 10 seconds will make a difference, for sure, as to when we end this meeting.

Some hon. members: Oh, oh!

Anthony Housefather: It's a pleasure to welcome all the witnesses.

With all of the different witness panels, we see a general tension between—

[*Translation*]

Claude DeBellefeuille: On a point of order.

[*English*]

The Vice-Chair (Frank Caputo): We have a point of order.

[*Translation*]

Claude DeBellefeuille: I think the majority of people are not wearing earpieces for interpretation. It's very difficult for me today, because all the discussions are in English. I can't work without interpretation. I'm a big fan of Mr. Housefather, but he speaks very fast.

Could he slow down so I can follow his questions?

I'm sure they'll be good questions.

Anthony Housefather: Absolutely, I will speak more slowly.

Claude DeBellefeuille: Thank you, Mr. Housefather.

[*English*]

An hon. member: There go your 10 seconds.

[*Translation*]

The Vice-Chair (Frank Caputo): Thank you, Mr. Housefather.

Anthony Housefather: I'll speak more slowly.

Claude DeBellefeuille: I don't want to take time away from you.

[*English*]

Anthony Housefather: Again, thank you all for being here.

I think we have a general tension in this law, as you've rightly pointed out, between the goal to be as safe as possible and the goal to respect privacy rights. We have to find the middle, where most people are comfortable. I don't think we'll ever find a situation where everybody agrees on the details of the bill, but I think we have to try to find that reasonable point.

We start from a premise that the bill is laudable in that it deals with some of the flaws in Bill C-2. The bill is really needed, in terms of law enforcement having access to information that technologically isn't dealt with under current law, but as everybody here said, there are concerns you have expressed.

I've noted a real discomfort with the idea of regulations. I would point out that there's a suspicion as to what's going to be in the regulations, and then we're hearing hypotheticals of what might be in the regulations or how orders might be used. Some people will trust the government and say that it will act reasonably, that the charter still applies and that there's still judicial oversight. Other people say that they won't trust it unless it's written in the bill. I get all that.

I also expressed concern about the interplay between systemic vulnerabilities and the orders. The way I read the bill, the company is exempt from having to do it if it creates a systemic vulnerability. I understand that we might need to look at the definition of systemic vulnerability. However, in an order, the company's obliged to carry out the order.

Mr. Geist, you talked about that issue. Could you express the way you would amend the bill to deal with that?

Michael Geist: I would highlight a couple of things.

First, it is essential that we get greater specificity around this issue, with more clarity around that definition. Many have expressed concern about what this could mean and the implications. This is serious in terms of what it means for our cybersecurity and for people's privacy, so I think we owe it to everyone to ensure that it becomes clearer.

Respectfully, I think there is good reason for people to listen to the debate and think that, in fact, some of those concerns are warranted. For example, during the House debate, I heard the Secretary of State for Combatting Crime talk about this being a first step. I walked into the hearing just before that, and the police officers were talking about wanting metadata for two or three years. Is that the next step—beginning to expand this into multiple years? I don't know, but there are real concerns.

In answer to your question, we need far more specificity around the definition to make very clear that this is not touching encryption and that there will be no orders that will create systemic weaknesses. That's a clear starting point.

● (1705)

Anthony Housefather: Basically, though, it's saying that proposed sections 5 and 7 are subject to proposed section 10. I also understand adjusting the definition of "systemic vulnerability".

Michael Geist: Yes, that was my other element. There were two: the definition and then this inconsistency we have in the bill that talks about, on the one hand, the ability to raise concerns, but on the other hand, language that suggests you have no real ability to challenge or to at least avoid an order.

Anthony Housefather: That one, I'm very sympathetic to.

I want to mention something, because I have less agreement with raising the grounds to "reasonable belief" from "reasonable grounds to suspect". I wanted to point out that the "Conditions for making [the] demand" say:

> (2) The peace officer or public officer may make the demand only if they have reasonable grounds to suspect that
>
> (a) an offence has been or will be committed under this Act or any other Act of Parliament; and
>
> (b) the confirmation that is demanded will assist in the investigation of the offence.

I think the combination there does create a situation where there is a reasonable burden, determined by the totality of the circumstances, that makes that threshold to be relatively reasonable in this context.

I understand, though, the idea of limiting what the production order could deal with, but should we do that, should it be, for example, this person's name and this person's address—all the stuff you used to be able to read in the telephone book—and not necessarily every particular service a person had, for example? Would you then agree that was a reasonable threshold? Yes?

That's for you, Professor Diab. I've already asked Mr. Geist this question.

Robert Diab: Thank you for the question.

I think there are two parts to this.

First of all, on the language you cited at the opening, the preamble, that's standard language. When it's challenged and courts are assessing whether it's a reasonable law under proposed section 8, they are going to be looking at the scope of it in addition to the grounds. One part of the whole question is this: Is "reasonable" suspicion too low even for just the name and address of the subscriber? That's one question left open in the wake of Spencer.

To reiterate a point that Professor Geist made just a couple of minutes ago, in Spencer the court said that we have a "high" privacy interest in the name attached to our subscriber information, because it ties us to a whole search history. It's a high interest. The court didn't say this. It was intimating that probably nothing less than a warrant on probable grounds would be reasonable, but it wasn't asked that question and it didn't have to answer—

The Vice-Chair (Frank Caputo): I'm sorry, Professor Diab, but I have to cut you off there.

[*Translation*]

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

Claude DeBellefeuille: Thank you, Mr. Chair.

Dr. Geist, you told us that retaining metadata for one year was too long and that 30 days would be a reasonable period. You specified that, if there is reasonable suspicion that there are criminal grounds, a warrant must be obtained to extend the retention period.

Did I understand your recommendation on this correctly?

[*English*]

Michael Geist: Yes. That was what I was suggesting.

In a sense, what I was trying to put forward is that there is always the ability for law enforcement, if it needs this information as part of an ongoing lengthy investigation, to seek the necessary order to have it preserved. The issue that law enforcement I think has identified in this context is that you don't know what you don't know in some circumstances, so you don't know that you might need it. There is this desire to build this giant haystack of information, because maybe you will need the needle at one point in time.

It seems to me that, of course, the haystack is comprised of people who have done no wrong. They're suspicionless. It raises for them real privacy-related concerns. Is there some kind of mechanism that we can find, in the spirit of trying to address law enforcement's concerns, that will allow, on a rolling basis, some of this information to be retained but quickly discarded after an appropriate period?

I heard in the last panel, I think, one of the members of law enforcement who was asked for a use case and talked about a missing person. Wouldn't it be good to be able to get that information? Respectfully, you don't need to retain everybody's metadata for a year for someone who's gone missing. I would think, frankly, that 30 days is more than enough to realize that the person is missing. Then, if there is a need to try to obtain other metadata, you can get the order to get it.

● (1710)

[*Translation*]

Claude DeBellefeuille: Thank you for your answer, Dr. Geist. That's pretty clear.

You know that Bill C-22 is important to us here. We all made a commitment to collaborate and, above all, to improve it. So if you have an amendment to propose or specific feedback to offer to improve it, I invite you to share it with us. All your suggestions are welcome, especially if you provide them in both official languages. They will be promptly forwarded to committee members.

Now, I'll ask you my other question.

Unless I misunderstood, I've learned that in Europe, data retention is limited to cases of serious crime, and that Europe is much more cautious when it comes to protecting privacy. In the United States, it's also not very clear whether metadata is retained for a very long period.

Do you consider that, in Bill C-22, Canada is more intrusive than its Five Eyes partners when it comes to retaining metadata?

[*English*]

Michael Geist: Europe has had a whole series of cases, both at the European level and at the national level amongst a number of member states, that have found some of the initiatives around mandatory metadata retention to be disproportionate. You get these cases, and countries begin to respond. It is a bit of a mix in terms of length and also under what circumstances and for what particular instances one might be able to retain that information, but it's very clear that European courts are uncomfortable with what I would characterize now as a Bill C-22–style metadata approach of retaining everything for a year. As you heard in the last panel, we don't see that retention at all in the United States. Clearly, it makes us out of step with some of those countries, but even perhaps more importantly, for the purposes of creating legislation that will sustain a potential challenge, I think it's out of step with where the charter is.

[*Translation*]

Claude DeBellefeuille: Law enforcement and government officials who have testified or approached us have told us that they want to align with the Five Eyes standards. Now, as I understand it, you're telling us that the measure providing for the collection and retention of data for one year is stricter and more demanding than what we see in the Five Eyes countries, and even more so compared to Europe.

Did I understand correctly, Dr. Geist?

[*English*]

Michael Geist: You can find examples where it's consistent, or otherwise. Again, we heard just before the talk about a lot of north-south-related issues with respect to crime. In the United States, we don't see these metadata requirements. In many European countries, we don't either. Canada would certainly be open to creating a system either without this at all or, if it did, for a very short period of time, working in conjunction with the ability to get quick-freeze orders to ensure you could retain it for longer periods. I see little reason to think that would not be viewed as doing our part as compared to our allies.

[*Translation*]

Claude DeBellefeuille: Dr. Geist, why do you think the government wants to give itself a great deal of regulatory flexibility in its definition of electronic service providers?

Why do you think it wants to retain this power?

[*English*]

Michael Geist: I wish I had a good answer. I mentioned off the top that this is an issue I've been focused on for decades now. My experience is that governments from both parties, whoever is in power, when working with law enforcement to flesh this out—

● (1715)

[*Translation*]

The Vice-Chair (Frank Caputo): I'm sorry, Mrs. DeBellefeuille and Dr. Geist.

[*English*]

The time is done.

Ms. Kirkland, your time begins now, for five minutes, please.

Rhonda Kirkland: Thank you, Mr. Chair.

Mr. Fraser, I appreciate your being here today. My questions will start with you.

Let me start with the difference between what's intended and what's allowable. I think most Canadians would not argue with the intention of this bill. Many times when we ask questions of the department, of both Justice and Public Safety, they rely on the statement, “Well, that's not the intention of this bill.” My concern is more about this: What does it allow versus what does the bill intend?

Yesterday, Public Safety Canada, on the social media platform X, posted this: “Fact or Fiction? Bill C-22 will require electronic service providers to create backdoors to their systems.

“Fiction! C-22 would not require backdoors.”

You responded on X, saying this: “Fact: There is nothing in Bill C-22 that would prevent the ordering of backdoors given the enormous powers granted under s. 5 and s. 7.”

Could you elaborate on that concern for the committee?

David Fraser: Absolutely, and I think that's one of the big issues with this bill.

With regard to the intentions of the bill, the bill is in two parts, and they do two very different things. One is about authorities, and the other is about capabilities.

If you look at clause 5 and the list of things that the Governor in Council can make regulations about, or clause 7 and ministerial orders, you see that they are written extremely broadly.

First, I would call your attention to the regulations that the Governor in Council may make. They include all the things in paragraphs 5(2)(a) through 5(2)(d), which means more than implicit granting of authority. Paragraph 5(2)(a) could include back doors, and paragraph 5(2)(b) could include back doors, because they can require the installation of devices on ESPs' infrastructure. There is nothing else in the bill that prevents that from happening, other than the goodwill of the minister and the goodwill of the intelligence commissioner, and that's that.

I am particularly very concerned about these secret orders, because the minister has the power to do any of the things that could be in a public regulation to any telco or any electronic service provider. At least the regulations are going to be published and will go through a process, and people can see them. However, secret orders can include back doors, because that certainly isn't precluded in the definition of “systemic vulnerability”, and it doesn't protect encryption in any meaningful sort of way.

If you take those two things together, the guardrails simply are not there. The only guardrail is the Charter of Rights and Freedoms, for which we'll have to have litigation in order to.... I'm afraid the government are setting themselves up for failure if they pass a bill that goes too far, a bill that violates the charter and that is going to be found to be unconstitutional. It's better to get it right.

Rhonda Kirkland: Thank you. We've talked about getting this bill right a few times, versus racing to just get it passed.

In terms of intention versus what's allowable, if the government truly has no intention of compelling back doors or weakening encryption, can you think of any reason not to clearly and explicitly prohibit those activities in the legislation itself?

David Fraser: I can't see any reason that we shouldn't include those guardrails. Guardrails are absolutely essential.

Part of the reality is that intention really doesn't matter today, because what is going to become law is what is written in that statute. The minister is going to change at some point and the government is going to change at some point, and we can see significant changing tides south of our border. If those powers exist in a completely different political environment, they can absolutely be used against the citizenry.

There is an expression, “turnkey totalitarianism”, which is something that causes me some concern.

Rhonda Kirkland: Thank you very much. I appreciate that.

Dr. Geist, in your May 2026 article, “Wilful Blindness?”—and there is a question mark on that—you argued that the charter statement that the Department of Justice requires the Minister of Justice to prepare largely ignored some of Bill C-22's most constitutionally vulnerable provisions.

In your view, why do you think the government avoided meaningfully addressing the sections of the bill that are most likely to raise serious charter and privacy concerns?

Michael Geist: I don't have a good answer for why they did it or why they didn't address those issues, but I will say that I think it raises real concerns.

If the reason is that they don't believe that issues around, let's say, mandatory metadata retention raise charter issues, so they felt there was no need to include it, I think that is both inaccurate as a matter of law and that it also suggests, as we've been saying, that this legislation is going to be challenged quickly. I think there is a real risk that provisions like that will be struck down.

● (1720)

Rhonda Kirkland: Thank you.

The Vice-Chair (Frank Caputo): Thank you, Professor Geist.

Next, we have Mr. Zuberi for five minutes, please.

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

Thank you to the witnesses for being here today on this important legislation.

I want to start with Professor Geist.

You were answering a question from a fellow parliamentarian, Madame DeBellefeuille, around privacy and how other Five Eyes and European countries handle that issue.

I'm also curious about judicial oversight and how Five Eyes and European countries approach judicial oversight with respect to a comparative analysis on Bill C-22.

Michael Geist: It's a good question. Candidly, I don't have a complete answer for you in terms of the production orders or the subscriber information that we've been focused on. Perhaps one of my colleagues on the panel does.

My area of focus has been primarily what happens in the network environment, in that intersection between providers and privacy, and that's where it feels like we're out of step.

Sameer Zuberi: Okay. Does anyone else have a comment on this? If not, I'll ask my next question.

We know there have been disproportionate impacts in policing with respect to racialized communities, indigenous people and different social movements. Do you have any concerns around impacts being different for specific communities within Canada in terms of this legislation?

Michael Geist: I could start, and perhaps others can proceed.

I have concerns, concerns that we've expressed. We do run the risk of undermining the trust—I referenced that towards the end of my remarks—between the public, their providers and, frankly, law enforcement itself.

When you talk about communities where some of that trust may have been, even now, strained, the notion that we are creating frameworks that lessen the safeguards that exist in terms of the standard to be able to obtain information, and even the base knowledge that, as people become more aware of the implications of some of these provisions, who they speak with on their devices, where they go and how they engage, all of that information being collected and retained for a year, I don't think knowing that their providers have this information increases the level of trust that people have with their providers. You're also then layering on top of that the fact that providers have been compelled to collect that information and then enveloping with secrecy what might take place with some of that kind of data. I think all of this undermines the trust that exists between the public and the various kinds of authorities whom we want to enhance the level of trust with.

Sameer Zuberi: Right. At some point, you have spoken about targeted quick freezes, instead of the current approach. Do you have any commentary? Do you want to expand upon that concept a bit?

Michael Geist: Sure. The basic notion between a quick freeze, which is, by and large, what takes place today, is.... We should probably just back up to note that there is no commercially viable reason for providers to retain metadata for long periods of time. There are risks. We've talked about those risks. Create that big haystack, so to speak, and you create a ripe target for hackers or others who might seek to gain access to it. It's a treasure trove, potentially, of information, but beyond that, it's expensive, which may render some providers less competitive, thereby increasing prices that Canadians face for their communications services, so by and large they don't do it.

What they do, though, is create a scenario whereby they will respond to orders requiring them to retain this information while an investigation is ongoing.

What I had suggested was this: Can't we find a way of marrying that system, which does allow us on that ongoing basis to retain that data, with a system that, for a very short period of time, if needed, allows for that retention and then gets quickly flushed? You can have it that in that very small minority of situations where you need that metadata retained for a long period of time, it's retained, but it's retained only where you have an active investigation, not against all Canadians.

● (1725)

Sameer Zuberi: In the 30 seconds that are left, do other European and Five Eyes have the approach as what you're describing?

Michael Geist: The quick freeze is the common approach that we find in jurisdictions that don't have mandatory metadata. It's not as if law enforcement can't get metadata in other places. They can, but with appropriate oversight, using that quick freeze model.

The Vice-Chair (Frank Caputo): Thank you very much.

[*Translation*]

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

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

Dr. Geist, I'll go back to my earlier question.

The bill fails to clearly define what an electronic service provider is.

Do you think there should be more clarity on what should be included or excluded in the definition of electronic service provider or in the definition of core provider?

[*English*]

Michael Geist: Yes. Mr. Fraser, I know, spoke to that, and he could perhaps elaborate around why that very broad definition encapsulates far more than I think most people would realize, given just how broadly it's defined.

I did want to return to your question that I didn't have the chance to fully respond to, where you asked, why go so broad? I do think—and I say this with respect—that as I look back on the many years of lawful access debate, it is invariably the case that law enforcement seeks as many powers as possible, and one can understand why. They would like to ensure that they can do their job as effectively as possible. However, just because you can demand that very broad approach doesn't mean that the government of the day ought to acquiesce, and certainly Parliament should not, once it's had the opportunity to study the implications and the trade-offs that exist when that happens.

We saw it, frankly, in Bill C-2, where there was clear overreach with respect to warrantless access to information from anybody providing a service in Canada. People said, hold on a second, that goes too far. Thankfully, the government listened on that issue, but we still have other issues where I think we need to recognize that it does go too far and we need to scale back, recognizing that we'll still address many of law enforcement's concerns and needs.

[*Translation*]

Claude DeBellefeuille: Perhaps you would agree to propose a way to limit the regulatory power this definition grants to the government. The only way to do so would be to specify what's excluded.

Isn't that right?

[*English*]

Michael Geist: I think, as a starting point, this notion of people engaging with information or information services in that way, as David Fraser noted, really does encapsulate everyone.

If what we're really talking about is that you have...and the vision is.... It's difficult, because it's just speculating. If it's just that core providers are the major telcos, but we're thinking about others that provide what might be viewed as parallel types of services, that's what I would have thought an electronic service provider might be, but that's not what we have in the definition right now.

The Vice-Chair (Frank Caputo): Thank you very much, Professor Geist and Madame DeBellefeuille.

Now we will go to Mr. Baber for five minutes, please.

Roman Baber (York Centre, CPC): Mr. Fraser, you're a lawyer in good standing with the law society of Nova Scotia.

David Fraser: I am.

Roman Baber: You've been practising for over 25 years.

David Fraser: As of last month, yes.

Roman Baber: You're a technology and Internet lawyer with the McInnes law firm.

David Fraser: That's correct.

Roman Baber: I also understand that you're a prominent speaker on technology and Internet issues. I came across one of your YouTube videos on this law that we're studying now, Bill C-22, on lawful access, and I'd like to provide the committee a quick transcript of your remarks:

"If Bill C-22, the lawful access act, 2026, becomes the law, the Government of Canada will be able to secretly order Apple to build in a capability into its infrastructure to allow Canadian law enforcement and national security folks to track every iPhone, every iPad, every Apple Watch, every Apple AirPod and every AirTag in real time. Then they'll be able to require Apple to confirm whether they provide you any services.

"Then [law enforcement] can go to a justice of the peace and get an order, without actually believing that a crime has been or will be committed, requiring Apple to hand over every device identifier for every device that you use with their services. That's the digital ID for your iPhone, iPad, Apple Watch, AirPod, Apple TV, AirTag. With that information, they can go back to the judge and get an order, again without actually believing that a crime has been or will be committed, requiring—

The Vice-Chair (Frank Caputo): Mr. Baber, please, if you could just slow down a shade—

Roman Baber: I'm almost finished.

"—requiring Apple to give them the moment-by-moment locations of all of your devices. Oh, and that secret order also required Apple to keep your location history for a full year, so cops can get that, too."

What's the problem, Mr. Fraser?

Voices: Oh, oh!

David Fraser: All of it.

Certainly, I have very few concerns with the judicial oversight. The threshold is obviously important.

However, if you take a look at all of these pieces as they go together, part 2 can require an electronic service provider—undeniably, Apple is an electronic service provider—subject to a secret order, to preserve metadata, location information, all that sort of stuff, and even build in new capabilities to their devices. That's under proposed paragraphs (2)(a) and (b) in clause 7.

Once that information exists, you can go to a judge and get an order on reasonable suspicion related to confirmation of service, then reasonable suspicion related to basic subscriber information, then reasonable suspicion in order to get the metadata and transaction information that they've been required to save.

This is potentially an entire package that we need to look at holistically and in detail.

● (1730)

Roman Baber: This is without actually believing that a crime has been committed, without swearing an affidavit saying, "I believe that a crime has been committed, and therefore, Your Honour, I get a court order."

I would like to dispose of some of the legal arguments that the Liberals make. I'd like to get specific, if I may, with Mr. Diab.

One of the arguments that is made on section 8, which is the arbitrary seizure.... What the government is proposing to do is to seize metadata, all of it, and order that it be held for 365 days, without knowing or suggesting that any offence has been committed. However, there's some jurisprudence on section 8—arbitrary search and seizure—that suggests that "seizure" requires a production. Here, we have no production.

How do you respond to that?

Robert Diab: The seizure is in the holding of it.

Roman Baber: Exactly.

Robert Diab: It's in the recording.

Roman Baber: The seizure is the fact that information is being held. The fact that it's not held by the cops but held on behalf of the cops by order of government is what makes it seizure, because you have government compelling the private sector to hold on to the information.

On to Professor Geist, it's very nice to see you in your non-Twitter persona.

Professor Geist, I have a major concern, specifically with the language of who can be bound by these orders. Specifically, it's the electronic service providers that can be compelled by a minister to design a system, a back door, etc. I looked at the definition of "service provider"—it's in section 2, "Definitions"—and it's basically anyone who provides electronic services to persons in Canada and does business in Canada. Then I went and I looked to see the definition of "electronic service", and it means anything "that involves the creation, recording, storage, processing, transmission, reception [or] emission" of electronic communication.

Well, it sounds to me like any law firm would be sending emails or receiving emails through its server, any bank would and any doctor's office would. We hear from the Liberal officials that only Internet companies are subject to this, but that's not what this legislation says.

Michael Geist: That's consistent with the question raised earlier, and no, that clearly is not what it says at the moment. It's clearly far broader.

If I might, you asked—

The Vice-Chair (Frank Caputo): I'm sorry. You were just about to give us a brilliant thought, Professor, but that brilliant thought will have to go to Madame Dandurand, if she so chooses.

You have five minutes.

Marianne Dandurand (Compton—Stanstead, Lib.): Yes, I would like to hear that brilliant thought.

The Vice-Chair (Frank Caputo): Let's hear the brilliant thought.

Michael Geist: I think it's way too hyped, at this stage.

Voices: Oh, oh!

I was going to say this: You asked a question with a long list related to Apple and the notion of, "Well, what's the problem?" The problem is, of course, all the data that might ultimately be retained and potentially accessed.

There is another problem here. Layering in some of these rules will mean that these companies may well either remove some of the services that protect Canadians—we've seen this with Apple in the U.K.—or choose to exit the market altogether if they are unable to meet the kinds of standards they expect of themselves and that their customers expect in terms of the privacy they provide. When you layer a very broad definition of "electronic service provider" in with very broad demands that may be inconsistent with where a company is at, you create an environment in which Canada may well be an outlier. Companies may stop providing particular kinds of protections or stop providing services altogether.

[*Translation*]

Marianne Dandurand: Thank you very much.

I'm going to let my colleague Mr. Zuberi ask you some brilliant questions.

[*English*]

Sameer Zuberi: I'd like to ask both Mr. Diab and Mr. Geist if they have anything they'd like to add they haven't yet had a chance to.

Robert Diab: Yes. I have one thought to put out on the hypothetical that has been floated a number of times to justify the metadata preservation power: the kidnapping of a 14-year-old girl, her trafficking, etc.

That is an effort to recycle something like the ticking-bomb scenario of 20 years ago. We heard a lot about the ticking-bomb scenario as a justification for torture. I want to be careful here, but the idea was about taking an extreme situation and using it to justify and normalize powers that are otherwise beyond the pale.

The committee should think about whether this is happening here. We're taking an extreme scenario—something that, if it does in fact happen, is very rare and unusual—and saying that all Canadians should give up a significant amount of freedom, security and privacy to enable law enforcement to be a little more effective in this remote scenario.

● (1735)

Sameer Zuberi: I appreciate that. I will continue along this path. If you can't comment, that's fine.

Right now, Canadians have a reasonable expectation of privacy when it comes to talking with a friend. It is a private conversation. The fact that it happens is a private conversation.

Can you comment on how our expectation of privacy would inevitably have to adjust because of this type of collection?

Robert Diab: When a law is challenged and a court is asked, "Does this allow for reasonable search and seizure?".... That's not the way they approach it. They stand back and ask, "When two Canadians are communicating in a restaurant, for example, would they think it's reasonable to assume that their conversation is private? If they are texting each other, would the reasonable Canadian assume that their texts are private?" That's the way they do it.

When this goes to the Supreme Court of Canada eventually, the question will be, “Would the ordinary, reasonable Canadian assume that the record of their texts over the past year, or the record of their movements, remains private?” in the sense that they were not recorded by the state for a law enforcement purpose, based on the potential that these random Canadians could have been committing a crime. Ask yourself that question. If you were a judge, would you think it's a stretch, or would you say, “Of course we don't want our movements recorded.”

Sameer Zuberi: With respect to this collection, there have been many concerns raised about its unintended capturing by unwanted actors.

Do you want to share any concerns about those we don't intend to have this information having it anyway, whether through the companies in question or hostile actors, be they foreign states, hackers, etc.?

The Vice-Chair (Frank Caputo): Answer very briefly, please.

Michael Geist: I'll respond this way. I appeared yesterday before a Senate committee on AI, where much of the focus was on cybersecurity. I have to say I find it positively dizzying going from one committee, where we're talking about things like Claude Mythos and the desperate need to ensure that we have cybersecurity that's as strong as possible, to then walking in and talking about legislation that would knowingly undermine that security.

Make it make sense—

The Vice-Chair (Frank Caputo): Thank you very much, Professor Geist. I apologize.

I want to exercise my prerogative as the chair, because there's one thing I think we're going to hear about in the next round that I think is very important. I'll ask you for a very brief, 15-second response.

You mentioned that 30 days for metadata would be appropriate. Oftentimes, there's not even an investigator assigned to an Internet luring case in 30 days. Bearing that in mind, what would you think about 90 days, given those types of crimes, to address those types of crimes or the metadata that would allow us to address those types of crimes?

Michael Geist: I guess the best way to respond to this is that too much of the policy-making associated with lawful access has not been evidence-based. It's based on the occasional anecdote without strong evidence.

It seems to me that if we are in the realm of trying to ask what the appropriate amount is—a year is clearly way too long—what we need is far more evidence, frankly, about when there are instances when that metadata is actually needed and how long it usually takes before you might be able to get that order.

The Vice-Chair (Frank Caputo): We will try to get that in the following panels. Thank you very much.

Thank you to our witnesses.

We will suspend briefly.

● (1740)

(Pause)

● (1745)

The Vice-Chair (Frank Caputo): We are now into our third panel.

I want to welcome our next panel of witnesses here to speak. We have, from the Canadian Centre for Child Protection, Monique St. Germain; from the Canadian Chamber of Commerce, David Pierce; and from the Peel Children's Aid Society, Mary Beth Moellenkamp.

Thank you, witnesses. You have five minutes each for an opening statement.

Ms. St. Germain, we will hear from you first, please. Thank you.

Monique St-Germain (General Counsel, Canadian Centre for Child Protection): Thank you very much, Mr. Chair and committee, for inviting us to participate in this study.

My name is Monique St. Germain. I am general counsel for the Canadian Centre for Child Protection, a national charity that works domestically and globally to reduce the incidence of missing and sexually exploited children.

We also operate Cybertip.ca, Canada's tip line for reporting the online sexual exploitation of children. In 2025 alone, we received 28,000 reports.

We also operate Project Arachnid, a platform that prioritizes the removal of harmful child sexual abuse and exploitation material. As of this month, Project Arachnid has issued 141 million notices requesting CSAM removal.

On a daily basis, our agency directly witnesses egregious privacy violations on children whose child sexual abuse material is circulating online for the world to view. We hear directly from children and families impacted by online crimes like CSAM, online luring and extortion. We welcome the measures in Bill C-22, particularly the confirmation of service demand and the subscriber information production order.

It's been over a decade since the Spencer decision left it open for Parliament to enact a reasonable law. We hope this time we can finally get there. In the intervening years, we have witnessed a number of growing threats to children, including an exponential increase in CSAM online. StatsCan figures show that CSAM incidents have quadrupled from 2014 to 2024. Then there's online luring. Reports to Cybertip.ca surged 344% between 2020 and 2025. StatsCan has this crime going up 65% in 2024 over 2023. Sextortion is another big issue. Cybertip.ca has received over 14,000 reports since 2020.

Even though crimes against children are through the roof, StatsCan data reveals that, in 2024, charges were laid or recommended in just 24% of all sexual offences against children online and in only 6% of CSAM incidents. We have to ask ourselves why.

This is obviously complex, but it has to be acknowledged that offenders are increasingly using sophisticated tools like burner phones, bulletproof hosts and VPNs, and networks like Tor that hide IP addresses. Some apps are blatantly and intentionally designed for anonymity. Offenders are able to rapidly change their digital identities through fake accounts. It's very common for offenders to use multiple apps, devices and accounts. Unravelling that web is incredibly complicated. On top of that, some of these investigations involve multiple jurisdictions and service providers. Record-keeping and co-operation amongst these providers varies widely. This has to be having an impact.

At our agency, we are now at the point where nearly one-third of contacts to Cybertip.ca or our support services come from children seeking help. These are just the children who come to us—often only when they are in crisis and, in some cases, suicidal. By the time these children feel able to reach out for help, the evidence that might help police identify their offenders could be gone. Even a single offender left unchecked can inflict an enormous amount of harm. Here is just one example: An Alberta offender posing as a female teenager was able to lure 92 children.

We wish to address one specific area of the bill that we would like to see changed. We believe the confirmation of service demand should include basic jurisdiction information, such as province and municipality. Having this information is critical, especially at the outset of an investigation when the available information is limited. Knowing the jurisdiction will help ensure that the right policing agencies are involved and that production orders are brought forward to the right court, and this can help police be much more effective in their investigation.

In closing, Canadian children have been forced to pay a very steep price as this debate rages on. Past failed efforts at lawful access reform are a powerful reminder of how long children and families have been waiting for action. We want police to be able to act. We need them to have the tools to do so.

Thank you.

● (1750)

The Vice-Chair (Frank Caputo): Thank you.

Mr. Pierce, you have five minutes, please.

David Pierce (Vice-President, Government Relations, Canadian Chamber of Commerce): Thank you very much for the opportunity to be here today on Bill C-22 and lawful access.

I am here as the Canadian Chamber of Commerce on behalf of our 400 network chamber partners and boards of trade across the country, our 200,000 combined members and more than 100 industry associations. I'm also here as a father. I can share that many representatives from Canada's digital companies also have families. We all want to ensure that law enforcement has the tools it needs to pursue criminals, especially online.

I'd like to express our appreciation to the Minister of Public Safety, the Minister of Justice and their teams for the extensive back-and-forth over the past year. The amendments made to Bill C-22 in part 1 addressed many industry concerns, and we thank the government for acting, but when you compare Bill C-2's part 15 and Bill C-22's part 2, it's clear that the government doesn't share the same concerns as the vast majority of our members at the Canadian Chamber of Commerce.

I've worked in and around cybersecurity for years. I don't understand why we treat cybersecurity differently from other crimes. If a business is hacked, the business CEO must apologize. The liability is on the business, even if the hackers are state-sponsored, yet our discussions here today are not about how we can support business to further protect their systems and our data. Instead, we're talking about obliging them to install devices, open their digital doors and give access to information to "authorized persons" essentially on demand.

● (1755)

[*Translation*]

The Vice-Chair (Frank Caputo): Mrs. DeBellefeuille, do you have a point of order?

Claude DeBellefeuille: The interpreter isn't able to do their job.

David Pierce: I'm sorry.

[*English*]

The Vice-Chair (Frank Caputo): Thank you so much.

Mr. Pierce, if you could, please speak a bit slower. We do have interpretation.

For all witnesses and all members, particularly when we're reading we do tend to read a bit faster. Please, everybody, just bear that in mind.

Thank you.

David Pierce: Absolutely, Chair, I'm happy to.

Let's imagine that this law is on the books. In a year or two, imagine hundreds and maybe thousands of investigations across multiple national law enforcement agencies and federal departments on all of our digital systems. Who's managing all those secure keys? Who's accountable for patching and updating those systems to make sure they are secure?

If I leave you with one message today, it's this. The business community supports production orders and we support urgent 24-hour production orders in exigent circumstances, but we are very concerned at the prospect of unfettered access by a government-authorized person to pull information from encrypted, secured systems.

What's also puzzling about this debate is that I've had the privilege of working with some of the most talented lawyers in the country, and there is a debate right now about whether or not Bill C-22 in part 2 requires a warrant. It is critical that the powers in Bill C-22's part 2 be amended to clarify this important point, especially in proposed subsections 5, 7, 14 and 20.

On the discussion of metadata, this will impose significant costs—millions of dollars—on businesses, and not just on the infrastructure to retain the data, but to manage it, to manage it securely and to have it in a usable format for law enforcement. As soon as you store large volumes of sensitive data, it becomes a cyber-target. As soon as data is retained, it's a target.

We recognize the importance of non-disclosure orders, but these should be limited to court-authorized actions tied to national security risks and active investigations.

Bill C-22 could also penalize successful Canadian companies that operate here in Canada but also have operations in the United States and Europe. If you are an electronic service provider based in Canada today, with customers in the United States and Europe, complying with parts of part 2 could put you offside with law enforcement and regulators in those jurisdictions. At a time when businesses are already facing tax competitiveness pressures, tariff uncertainty and the broader economic risk that we're all facing, adding another layer of regulatory burden on Canadian companies at this particular time may incentivize them to relocate.

Finally, with regard to the definition of “core provider”, without an amendment to this section, it potentially captures the vast majority of Canadian businesses that communicate or provide an electronic service.

In closing, the business community very clearly has signalled that they're concerned about Bill C-2 and part 2 especially. I think we all trust that the current Prime Minister, the Minister of Public Safety and the Minister of Justice will use the measures in this law in a way that's appropriate and as they've said. I'm sure the public servants who were at the committee on Tuesday would do the same. They seemed to be very honest and reputable—

The Vice-Chair (Frank Caputo): Thank you very much, Mr. Pierce.

We'll now move on to Ms. Moellenkamp for five minutes.

Mary Beth Moellenkamp (Chief Executive Officer, Peel Children's Aid Society): Mr. Chair and members of the committee, thank you for the opportunity to appear. My name is Mary Beth Moellenkamp, and I'm the chief executive officer of the Peel Children's Aid Society.

Peel Children's Aid is a mandated child protection agency for Peel Region, including child protection responses connected to Toronto Pearson Airport. We also lead, alongside our partners, nCourage, Peel's anti-human sex trafficking integrated service hub, and CWICE, the Child Welfare Immigration Centre of Excellence.

Through this work, we see how trafficking, immigration, housing instability and cross-border movement intersect with child safety and reflect broader provincial and national trends. That experience gives us a particular perspective on Bill C-22.

Bill C-22 responds to a real challenge: whether lawful systems can move quickly enough to protect children in a fast-moving, digitally enabled environment. Children can be groomed, isolated, threatened, moved and controlled through digital tools faster than systems can identify risk and respond. Timely, lawful access to digital evidence can help find a child, identify the adult causing harm, prevent further exploitation and support coordinated intervention.

At the same time, safeguards are essential. The use of these tools must remain grounded in lawful authority, appropriate oversight, clear thresholds, privacy protections and respect for children's rights and dignity.

The child welfare system holds a difficult but necessary tension. We are responsible for protecting children from harm while also protecting their privacy, voice and civil liberties; and both matter.

Children and youth involved with child welfare often already experience high levels of system involvement. They are disproportionately represented among victims of sexual exploitation and trafficking. Many have experienced trauma, abuse, neglect, instability and disrupted relationships.

Traffickers exploit these vulnerabilities. What begins as connection can quickly become coercion and control. Some youth are drawn into other forms of criminal exploitation, including auto theft, fraud, drug movement or recruiting other youth. These children are often being manipulated, threatened and isolated.

In Ontario, as in other jurisdictions, human trafficking is recognized as a child protection concern. We have a clear role in assessing safety, supporting caregivers, collaborating with police and community partners, and protecting children from ongoing harm. Increasingly, our efforts focus on identifying traffickers and exploiters as the individuals causing harm rather than viewing parents and caregivers as failing to protect.

Traffickers exploit gaps between systems and jurisdictions. They exploit delays and digital platforms that move faster than our legal and service responses. The average age of recruitment into sex trafficking is estimated to be 13 years old.

At Peel CAS, we have supported children as young as nine years old. Last year, our agency identified more than 200 cases where a child or youth was suspected of involvement in trafficking for sexual exploitation, and yet we know that this is significantly under-reported. Often a child may only know a trafficker through a phone number, social media handle, app, vehicle, hotel or email address. Those fragments matter. They may be the difference between not knowing where to look for a child and locating a child.

The value of Bill C-22 for child welfare is indirect, but it's important. It may help our police partners obtain lawful digital leads that child welfare agencies, trafficking hubs, survivor services and community organizations can translate into safety planning, protection and survivor-centred support. Exploited youth must be treated as victims and survivors, not as offenders.

Digital information alone will not make children safe. Safety requires coordinated systems, including child welfare, police, survivor-led supports, indigenous and culturally specific services, immigration expertise, housing and mental health supports. Used lawfully and with safeguards, Bill C-22 may help partners locate children sooner, disrupt exploiters faster and strengthen collective efforts to protect children and youth.

Thank you.

● (1800)

The Vice-Chair (Frank Caputo): Thank you very much, Ms. Moellenkamp.

I want to thank this panel of witnesses.

I will begin the first round of six minutes now.

Ms. St. Germain, you probably don't remember me, but I consulted you when I was writing the bill to change the name from child pornography to child sexual abuse and exploitation material. I first became acquainted with your work when we both attended the same B.C. ICE provincial strategy conference. For those who don't know, the RCMP in Vancouver has a specific unit that investigates Internet and child exploitation. People from all sorts of agencies gathered at the conference. I really appreciated your interventions there.

One thing we were talking about in the prior round was how long it takes for an investigation to kick off. I have prosecuted an Internet luring case. A lot of people don't realize this, but the software for a service provider, let's say, Facebook, could pick up an attempt to lure a child. Then, that goes to Washington, D.C., as I recall—it used to anyway—to the National Center for Missing & Exploited Children. I believe it would then go to the national headquarters for the RCMP, and then it would go to the province. Is that somewhat accurate?

● (1805)

Monique St-Germain: Yes, assuming this is coming through mandatory reporting in the United States.

The Vice-Chair (Frank Caputo): Yes, exactly.

Monique St-Germain: That is how it goes.

The Vice-Chair (Frank Caputo): That process takes a fair amount of time. I asked one of the legal experts on our previous panel about this. When we're talking about data retention, how long do we need to retain data? I don't think anybody thinks data should be retained indefinitely. You're a lawyer. You understand where people are coming from. We also have to look at how long data needs to be retained in order to have an investigation.

In your experience, can you tell us how long it takes for an investigation to kick off to the point where somebody would look at it and say that they need something? For example, it could be a missing IP address that is an evidentiary gap, and if they were to have it, this would help them catch a child predator. Hopefully, I'm being clear.

Monique St-Germain: Yes, I understand what you're asking. I'm not sure that I'm the person you should be asking. We're not police. The role we play is very distinct and separate from police. We get tips from different places and pass things on to police, but then the investigative process they follow is within their knowledge.

We know, from where we sit in the continuum, oftentimes when the tips are coming in to us from Canadian children and families, that they can't be acted upon. By the time the information gets through to police, there may not be sufficient information for them. There certainly have been delays, in terms of getting subscriber information, to link the information they have to an actual location so that they can start to investigate someone.

For an example, an IP address may lead to an individual house, but within that house, there may be four individuals living there. There's a whole process. Every step in the process helps narrow down and get closer to the actual person.

On the issue of metadata, what I understand from the bill is that this is being left to regulation to go through what metadata is being captured, being saved and being saved for how long. That is an important process in order to clarify what pieces of information are going to be helpful. Certainly, from what we see in the courts, that information is critical in terms of linking an offender to a particular piece of activity on the Internet.

The Vice-Chair (Frank Caputo): I appreciate that.

One of the greatest challenges I saw was linking the person in the prisoner's box to the person behind the computer screen or on the phone because you must have a piece of evidence that is linked in every spot.

How long does it generally take from the time you get a tip to the point where something can be sent to a police agency?

Monique St-Germain: Our role is to turn the tips around as quickly as possible. We will process the information, and if it appears to reveal that it is a criminal act, then we will send it to the police agency that we believe has jurisdiction.

We will use tools to try to figure out what we can, based on what we have. We're not necessarily getting things like IP addresses or anything like that. We're getting what the child is saying, such as the username of the person or the description of what is happening. We're trying to get the police where the child is, unless we can figure out something about the offender.

We turn it around fairly quickly. Within 48 hours, if not sooner, we will have something turned around. We certainly try to prioritize things and get through everything very quickly.

The Vice-Chair (Frank Caputo): That username is then used to get a production order, ideally, on oath or on affirmation, which is part of what this bill is about.

Ms. Moellenkamp, do you have anything to add to this, based on your expertise?

Mary Beth Moellenkamp: Can I ask you to repeat the question?

The Vice-Chair (Frank Caputo): I was just asking how long it takes, in your experience, to kick off an investigation. Do you have any experience with how long it takes? I know you're not a police officer, but I'm trying to gauge that.

Mary Beth Moellenkamp: In the child protection system, we have eligibility that we consider around the level of risk to a child. We may determine that we need to go and see a child within 12 hours, or we may determine that the risk is more moderate and are required to see them within seven days. For the 12-hour response, often, we are working alongside police. There are regulations under our act to do joint investigations.

I have seen some challenges around getting data to address this—to find out where a child may be, especially if we're looking for a missing child or at an Amber alert. We have had situations where it's been difficult to get that. The police are waiting to get an order. They're not able to do that quickly enough.

● (1810)

The Vice-Chair (Frank Caputo): Thank you. I apologize for cutting you off, but we have to move on to Mr. Ramsay for six minutes.

[*Translation*]

Jacques Ramsay: Mr. Pierce, as it happens, you are in the company of two people who deal with cybercrime, among other things.

Among other things, you have heard about a defendant who made 92 children aged 9 to 13 his victims. We're talking about over 200 calls per year. Law enforcement urgently needs the powers required to be effective. The rapid-fire approach doesn't work in this case. As you've heard, reports are often made several months after the offence has taken place.

Given that, how do you reconcile your requests with the needs, taking all that into account?

We're talking about child sexual abuse, but we could also be talking about extortion targeting businesses. Recently, there have been repeated incidents in Surrey and Brampton. So it's urgent that complete information be provided in a timely manner. I'd like you to tell me how you reconcile that with your requests.

[*English*]

David Pierce: I will start from a cybersecurity perspective.

I don't think it makes anybody safer if our systems are compromised. That's a fundamental point. All of your data, my data and our families' data.... It's about financials, pictures or whatever the case may be, including location data indicating when you're not home so your house can be broken into. Our whole world is digital. If we lose encryption on these major systems, it will be a fundamental risk to the Canadian economy. It will be a fundamental risk to businesses being successful in our country. It would put us out of step internationally with countries where the systems of large providers that provide these services would be at risk.

From a business perspective, I think it's critical to remember the context we're in right now. These are not smooth economic times. In the case of large providers, you're talking about adding millions of dollars of additional expenses to their balance sheet. What about the smaller businesses and electronic service providers across the country that fill gaps the large ones do not fill? They don't have the capacity to pivot and finance large operations to essentially support law enforcement coming in and attaching a device to the back of their system, and to work with them over a long period of time to facilitate this.

I'll go back to my opening comment, if I can.

We all want law enforcement to have tools that are effective. We all want law enforcement to be able to pursue the criminals and protect our kids and families—all of us. It's really important that the measures this bill would provide are balanced between protections for our data and privacy with, above all else, protections for our encrypted systems.

Jacques Ramsay: All right.

[*Translation*]

The bill also provides for a prohibition on—

[*English*]

There's a prohibition against electronic service providers implementing a capability that would introduce a systemic vulnerability. Somehow you don't feel that this is enough.

David Pierce: I'll give you an example. I watched the testimony on Tuesday. One of the officials made a comment that in many of these systems there are two keys, so we can just have the providers issue a third key or another key that we can use.

Cybersecurity is not just technology. Cybersecurity is equal parts technology and humans. The human interaction with technology...I'm sure everybody knows someone who opened an email that let some virus into your system. The question is, who's managing those keys? Who's protecting those keys? How are those keys protected? Who has access to them? Keys change. Who's updating those keys? Who's doing the patches on those systems?

Look at FINTRAC. Look at some of these large Salt Typhoon hacks, in which these are very sophisticated actors. It's funny: I go back to my opening comment, when I expressed a bit of frustration, just because cybersecurity is looked at differently from every other crime. The real hackers of today are not in a basement in one of our major cities. They're foreign adversaries. They're state-sponsored. These are sophisticated operations. If you'd just add a new door to the back of the system, they will have been there on Monday. If the door appears on Tuesday, they're going to say, “Hmm, that looks different. It doesn't look like the other doors.” They'll start to probe it, and that immediately becomes a target.

Again, I go back to the point that the whole concern from the business community is, one, about encryption and making sure these systems are protected; but, two, about ensuring that we have the ability to conduct commerce and that we can have trust that our systems and our information is safe. If the measures in Bill C-22, part 2, are implemented as written, the language does not preclude the concerns I've just outlined.

● (1815)

[*Translation*]

The Vice-Chair (Frank Caputo): Mrs. DeBellefeuille, you have the floor for six minutes.

[*English*]

Thank you, Mr. Ramsay.

[*Translation*]

Claude DeBellefeuille: Thank you, Mr. Chair.

My question is for the Canadian Chamber of Commerce representative.

At a time when U.S. tariffs are creating significant instability for our businesses, do you believe that not knowing which businesses are subject to the access to information law leads to an inability to predict the future, which can harm business?

[*English*]

David Pierce: Absolutely. I'll share, quite honestly, the discussion in industry when this law was first introduced. Many thought that they were excluded, simply by the fact that they weren't defined as electronic service providers. However, when you really look into that definition, it's providing an electronic service. What do you use today that doesn't use some form of electronic communication? My car does that. We have so many different devices and pieces of equipment. It's not typical to just narrowcast it to one small subset with the language that's in the law.

Our suggestion is that there be a primary function test, applied to the definition of a core provider, that narrows it down to companies that are specifically in the business of communication, which is ultimately what I believe law enforcement is after. However, if it is left as it is right now.... As we were going through this with our members across the country, initially the industries thought they were excluded. Then they went back, looked at it and said, “Well, geez, you're right. This could capture us.” That ambiguity really should be closed in this process, we hope.

[*Translation*]

Claude DeBellefeuille: Do you think Quebec and Canadian companies are ready to meet the requirements of Bill C-22?

Are any of your members saying they're ready? Honestly, Mr. Pierce, I believe the bill will likely be passed, even though we hope it will be improved.

Do you consider it will take an enormous effort to prepare to meet the expectations imposed by Bill C-22? Is it costly?

You told us that this has economic consequences. Have you quantified them?

Have you assessed what it will cost to comply with the expectations and requirements of the bill?

[*English*]

David Pierce: I'll start with the cost piece and then I'll work backwards from there.

For large providers, the cost is in the millions to set up the infrastructure to comply with this, and then millions more in operational costs. It's very important to remember that metadata is not something you can just go in and read. It has to be in a usable format that law enforcement would find useful and helpful.

The bill is in two parts. I believe the clerk will be distributing an English and French letter from the chamber of commerce to members in which we've identified areas where we think both part 1 and part 2 need to be improved. We understand the Spencer decision. On part 1, with the changes that were made and the changes we've recommended in our letter, perhaps there's an opportunity to split the bill so that part 1 can move forward and deal with some of the concerns that I know my other two colleagues on the panel spoke to so eloquently earlier, and we can study part 2 a bit more.

From my perspective, when you look at authorities in proposed sections 5, 7, 14 and 20... The number of lawyers I've talked to over the past year who said they cannot rule out whether or not a warrant is required says, to me, this might need some more study and it might need some more work. I would hate for it to be passed in order to resolve what part 1 is after and then create a host of trade and business issues for the economy as well.

● (1820)

[*Translation*]

Claude DeBellefeuille: If the government had had a majority, Bill C-2 would have been passed, despite unanimous opposition. The government did a better job drafting Bill C-22 and it held consultations. Therefore, honestly, I'm not very supportive of your suggestion to split the bill in two.

Do you have any highly specific amendments that you could share with us that would, for example, reduce the impact on businesses, or that could help them transition and comply with the requirements set out in Bill C-22?

Given that you've consulted with many lawyers, I imagine you must have some improvements to recommend. Do you have any specific suggestions?

[*English*]

David Pierce: I thought you would never ask. Absolutely, we would be happy to submit amendments to correct the legislation to address the concerns I've outlined. In particular, you'll find on the back the letter that will be distributed—I presume by the clerk at some point—that we've identified the issues, issue by issue, in part 1 and part 2 and then in both parts of the bill. That's obviously what we would use as a guide to develop those recommendations.

Thank you for the offer.

[*Translation*]

Claude DeBellefeuille: The deadlines for reviewing Bill C-22 are quite tight, and as members of the committee, we must submit our amendments by May 27. I just wanted to let you know that any suggestions for improving Bill C-22 are welcome.

I'd also like to thank you for speaking on behalf of businesses. We have a diverse range of witnesses, and that's what allows us to get a better idea of the improvements that need to be made to the bill.

Thank you very much, Mr. Pierce.

The Vice-Chair (Frank Caputo): Thank you, Mrs. DeBellefeuille.

[*English*]

For the benefit of the committee, we have been running a bit late. It's not because we have not been efficient, but because we have had more opening statements than we are used to.

What I would propose, to ensure that we give our next panel the appropriate amount of time, is to now have a four-minute round for the Conservative Party and a four-minute round for the Liberal Party, and then move on to the next panel so that we can finish on time. I hope that is okay.

We will move to Mr. Lloyd for four minutes, please.

Dane Lloyd: Thank you to the witnesses.

Hello, Mr. Pierce. It's been a while. It's good to see you.

David Pierce: Hello, sir.

Dane Lloyd: I was wondering if your stakeholders in the business community would be satisfied with a more specific definition of the term “systemic risk”. Would it allay some of their concerns?

David Pierce: Very much. Especially listening to the testimony on Tuesday, the key is that the legislation specified that it's not about just creating a systemic vulnerability that service providers will not be required to break encryption. That's a very important principle that is assumed with the current definition, but we believe it should be very clearly codified in law to address the concerns of the industry.

Dane Lloyd: Dr. West was talking about how these powers should be administered by the businesses and the operators themselves, not by law enforcement. Is it your understanding that it would be preferential?

David Pierce: I go back to my comment in the opening statement.

I believe the business community is fully behind exigent circumstance and quick turnaround production orders. They know their systems. They know where the data is. They know how to pull it and produce it in a way that can be useful and, at the same time, not create that vulnerability that we've been so clear about.

Dane Lloyd: One concern I have is if law enforcement comes to one of your stakeholders, an operator, and says that it needs access to the system. The company is going to ask for a warrant or ministerial order. If law enforcement is given the capabilities through a ministerial order to have direct access to the systems, what safeguards are there to ensure that maybe some bad actors aren't using that access?

We've seen that in some cases there are allegations of people in law enforcement looking up ex-spouses and things like that. What guarantees can we add to this legislation to ensure that some bad actors aren't going to use this trove of new data in an abusive way?

● (1825)

David Pierce: There are bad actors, and there is corporate espionage by competitors. The intellectual property of these companies is incredibly valuable. To give unfettered access for someone to peruse as they see fit is a great risk.

Our biggest focus, as I mentioned previously, is that we believe production orders are the way to go. That is the most clear option.

Dane Lloyd: Thank you.

I want to get a quick question in to Ms. St. Germain.

[*Technical difficulty—Editor*] The integrated childhood exploitation centres were telling me about how many of their child exploitation investigations were shut down because they primarily rely on tips from the FBI.

Does this legislation fix the problems created by the Bykovets 5-4 decision?

Monique St-Germain: I didn't hear the first part of your question. There was no sound coming through.

Dane Lloyd: I was told by the integrated childhood exploitation centres that many of their tips come from the FBI. Were they shut down because of the Bykovets decision? Does this legislation fix that issue?

Monique St-Germain: It helps.

Part 1 has the provisions about voluntary provision of information and clarifies that police can use information that is voluntarily provided. A lot of the tips that are coming from the National Center for Missing & Exploited Children in the U.S. are voluntarily provided. Those are coming through and are then being sent over to our police forces. In some jurisdictions, there is some uncertainty as to whether or not the police can actually use that information to then start the investigation.

The parts in part 1 that are talking about the “for greater certainty” provision and the clarification about voluntary information, yes, will help.

The Vice-Chair (Frank Caputo): Thank you.

Ms. Acan, you have the final four minutes, please.

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

I will go with Mr. Pierce for my first question.

The open letter that we received raises some concerns that the orders could be used to obtain sensitive medical or financial records.

Can you explain for the committee that proposed subsection 487.0121(3) in the bill creates an explicit prohibition against making any demand that would disclose medical information or solicitor-client privilege?

David Pierce: I'm sorry. Is this with regard to part 1 or part 2?

Sima Acan: This is in part 1.

David Pierce: I apologize. I'm not familiar with that specific section. If I can come back to you with that afterwards, that would be great.

Sima Acan: No worries.

I will continue my questions with CCCP and the Peel CAS.

I have volunteered countless hours over many years, supporting organizations like SAVIS of Halton. SAVIS serves as a leading agency in my region of Oakville. It's a backbone organization for the Halton Collaborative Against Human Trafficking, which brings together community organizations and partners to create a coordinated regional response to combat human trafficking. It's an organization such as yours.

Organizations like yours play a critical role in protecting vulnerable individuals and in strengthening community awareness and prevention efforts. Unfortunately, traffickers have frequently used Oakville and Burlington as transit hubs because of their proximity to major highways, moving victims between hotels along these corridors in an effort to avoid detection.

We are fortunate to have the dedicated members of our Halton Regional Police Service. I want to sincerely acknowledge and thank them for their continued work in combatting these horrific crimes.

Over the past year, I have spoken with many officials from different levels of law enforcement, and they have consistently emphasized that the child exploitation investigations are extremely complex and time-intensive. These cases can often take more than six months to resolve, particularly due to criminals' use of phones, computers, cloud services and storage devices to conceal illicit material.

From your perspective, how would Bill C-22 improve law enforcement's ability to investigate and combat child exploitation and human trafficking offences?

● (1830)

Mary Beth Moellenkamp: Bill C-22 would help law enforcement access this information more quickly. We sometimes have minutes or hours when we're looking at an investigation and trying to protect a child.

I want to speak from a Pearson airport perspective.

Sometimes we have children and youth coming through the airport who have been identified. Being able to access that information and look at that digital footprint is important because, once they go through, we may have no other opportunity to see that child again, and we may not know where they end up.

You rightly said that, within the GTA, there are many different transportation routes from the highways to the airports. This creates some challenges. Accessing that quickly is extremely important because time is of the essence in those cases.

Sima Acan: Thank you very much.

Madame St. Germain, do you want to add anything to that?

Monique St-Germain: I will say that, in particular, the provisions in part 1 would be very helpful because a lot of child sexual exploitation investigations involving a tip from a provider, through NCMEC or something similar, have very minimal information. Police can't really do a lot with that information until they can get a bit more. The information demand, coupled with—

The Vice-Chair (Frank Caputo): Thank you, Ms. St. Germain. I apologize, but I have to cut you off. I'm really sorry. We are running late here.

Sima Acan: Five minutes is too short.

The Vice-Chair (Frank Caputo): Witnesses, I encourage all of you, if you wish, to provide supplemental information to the committee. You all play a critical role. On behalf of the committee and all Canadians, we are grateful for your work. Thank you very much.

We will suspend for as short a time as possible, preferably 90 seconds.

● (1830)

_____(Pause)_____

● (1835)

The Vice-Chair (Frank Caputo): We're back.

I apologize if that was a bit aggressive. I want to thank all panellists today. They are excellent, and we have a very distinguished panel. I really don't want to lose any time with them.

I want to introduce them.

We have, from Meta Platforms Inc., Rachel Curran and Robyn Greene. From NSIRA, we have the Honourable Marie Deschamps, Craig Forcese and Lawrence Mangano. Finally, we have the Honourable Simon Noël and Justin Dubois.

We will now have opening statements.

I have to vacate the chair for about three minutes. If anything comes up, Madame DeBellefeuille will deal with it. I will hopefully be back in three or four minutes. If not, please go on to the next opening statement. Thank you.

We will start with the opening statement from Meta.

Rachel Curran (Head of Public Policy, Meta Platforms Inc.): Thank you, Mr. Chair.

Good evening, and thank you for the opportunity to appear before the committee today. My name is Rachel Curran. I'm head of public policy for Canada at Meta. Joining me is my colleague Robyn Greene, who is an expert in the subject matter under consideration. Please direct your technical questions to her.

Meta is deeply committed to keeping our Canadian users safe online and off-line. We routinely engage with Canadian law enforcement agencies at all levels of government, including by proactively reporting threats we identify or by responding to valid legal demands and emergency requests from Canadian authorities.

We commend the government for addressing many of the concerns that were raised about part 14 of Bill C-2. With narrowly tailored amendments, we think the current part 1 of Bill C-22 would provide law enforcement with an effective legal framework for obtaining the necessary data in a timely manner. However, part 2 is a different story and could ultimately make Canadians less safe, not more.

First, the technical assistance obligations in part 2 could conscript private companies into service as an arm of the government's surveillance apparatus. As drafted, the bill could require companies like Meta to build or maintain capabilities that break or undermine encryption and force providers to install government spyware directly on their systems.

The bill purports to protect against risks to encryption by allowing providers to challenge demands that would introduce a "systemic vulnerability". However the definition of "systemic vulnerability" is unclear. Essential terms like "encryption" are left to be defined in regulation, while ministerial orders can override those same regulations. Moreover, the bill contains no process for challenging a problematic order, or liability protections for companies while a challenge is pending.

The technical community's consensus on this is clear. It is not possible to build back doors to encrypted systems for law enforcement without creating vulnerabilities that will be—not could be, but will be—exploited by malicious actors. Weakening encryption does not just affect the target of an investigation. It affects every Canadian who depends on secure private communications to do banking, access health care, run a business or simply talk to their family.

This is not a hypothetical risk. Governments around the world are still dealing with a fallout from China's state-sponsored Salt Typhoon cyber-attacks, which exploited the U.S.'s far narrower technical assistance laws. Canada's own security agencies understand this and issued guidance that specifically advised adopting encryption to defend against these kinds of cyber-attacks.

Part 2 of Bill C-22 would move Canada in the opposite direction and out of step with our closest allies. Last year, France and Sweden both abandoned similar proposals, and the EU guaranteed robust encryption protections in its agreement on online safety. The U.K.'s use of a similar authority ordering Apple to break its encrypted cloud service drew condemnation from the U.S. government and 200 global civil society organizations, and ultimately resulted in Apple withdrawing its advanced data protection service.

Imposing these obligations would also chill domestic innovation and investment and harm Canadian competitiveness abroad.

In addition, overly broad non-disclosure orders in part 2 risk undermining public trust and transparency. The bill's data retention provisions would create a framework to capture the private information of ordinary Canadians with no connection to any crime, and also grant warrantees the authority to search company premises and seize data.

In light of these significant challenges, we urge policy-makers to separate part 2 from Bill C-22 so that these critically important issues receive the time and attention they deserve.

To avoid the worst privacy and security outcomes, required changes include removing obligations for companies to add government or third party surveillance tools or other software to their systems, and strengthening the definition of “systemic vulnerability” to explicitly rule out any requirement that would weaken or break encryption, and codify the process for companies to challenge requests.

● (1840)

Thank you, Mr. Chair.

The Vice-Chair (Frank Caputo): Thank you, Ms. Curran. I apologize, but I have to be ruthless with the time.

[*Translation*]

Ms. Deschamps, you have the floor for five minutes.

Hon. Marie Deschamps (Chair, National Security and Intelligence Review Agency): Mr. Chair, members of the committee, good evening.

Thank you for inviting us to participate in your work.

I am chair of the National Security and Intelligence Review Agency, or NSIRA. I am joined by our vice-chair, Craig Forcese, and our secretariat acting executive director, Lawrence Mangano.

[*English*]

I'm going to use this time to make two points.

Given the scope of the new powers being proposed in this bill, timely and effective independent review is essential.

[*Translation*]

That's my first point.

[*English*]

Second, this bill, in its current form, falls short of supporting that review.

[*Translation*]

NSIRA has two core responsibilities. First, it reviews national security and intelligence activities to assess whether they are lawful, reasonable and necessary. This should not be confused with the authorization granted by my colleague Mr. Noël, which he will tell you about a little later.

Second, NSIRA investigates public complaints related to national security and intelligence.

[*English*]

In doing so, we provide independent assurance to Canadians that those activities comply with the law, including with the charter. Bill C-22 introduces significant new powers through the proposed supporting authorized access to information act. Given the breadth of these new powers, NSIRA anticipated a review role that would provide timely and direct visibility into how these authorities are used.

[*Translation*]

However, as drafted, Bill C-22 only provides NSIRA with the minister's public annual report. In practice, this could mean delays of more than a year before NSIRA becomes aware of how these authorities are used.

● (1845)

[*English*]

While NSIRA has broad access rights, there is a real benefit in legislation that requires information to be provided proactively to NSIRA in a timely manner. In the context of constrained resources, early awareness would provide a meaningful baseline of what activities are taking place and allow NSIRA to plan and target its reviews more efficiently.

[*Translation*]

We do welcome the requirement for intelligence commissioner approval of ministerial orders. However, the absence of provisions granting NSIRA access to those orders, or information about how they are implemented, limits our ability to assess their use in practice.

To address this, we recommend two targeted amendments.

[*English*]

The first is to amend proposed section 9 to ensure NSIRA is proactively provided access to classified ministerial orders issued to service providers as well as to information provided to the intelligence commissioner in support of those orders.

The second is to amend proposed section 27 to ensure NSIRA is informed when compliance orders are issued, including information relevant to potential non-compliance. These changes would enable more timely, targeted and effective reviews.

[*Translation*]

Furthermore, these amendments are consistent with existing Canadian legislation, where NSIRA receives proactive information related to activities conducted under ministerial authorization, and with international practices.

Australia also has provisions of this nature. You can ask questions about that.

[*English*]

In closing, independent review is a cornerstone of public trust in Canada's national security framework. Ensuring that NSIRA has timely access to relevant information will strengthen accountability and support Parliament's intent in establishing these authorities.

[*Translation*]

Thank you for your attention.

We would be pleased to answer your questions.

[*English*]

The Vice-Chair (Frank Caputo): Madam Deschamps was on the Supreme Court of Canada when I was a law student. I just can't cut her off.

Voices: Oh, oh!

[*Translation*]

The Vice-Chair (Frank Caputo): Mr. Noël, you have the floor for five minutes.

Hon. Simon Noël (Intelligence Commissioner, Office of the Intelligence Commissioner): Thank you, Mr. Chair and members, for the invitation.

I am accompanied today by Justin Dubois, executive director and general counsel at my office.

Bill C-22 gives my office a new and significant function. I want to explain how this function would fit into my existing duties.

[*English*]

My quasi-judicial function as intelligence commissioner, or IC, is to approve or not approve certain national security and intelligence activities proposed by CSE and CSIS, and authorized, respectively, by the Minister of National Defence and the Minister of Public Safety.

My independent approval is necessary because the activities that the ministers authorize may be contrary to the law or breach the reasonable expectation of privacy of all Canadians. I have 30 days to render my decisions, but I adapt to much shorter timelines when urgency calls for it. Only with my approval can the activities be conducted.

When I approve a ministerial authorization, I assess whether the minister's conclusions are reasonable in light of the factors the legislation requires the minister to consider, including the impact on privacy interests and cybersecurity. For most of my decisions, my primary concern is how the proposed activities impact the privacy of Canadians. I apply the legal principles of proportionality and reasonableness, and I ensure compliance with the charter, including section 1.

● (1850)

[*Translation*]

In this regard, when I look at the factors the minister must consider when issuing an order under this bill, I am confident that these orders are similar to the ministerial decisions I currently oversee, and raise legal issues my office is well versed in.

In my experience as intelligence commissioner, I understand how certain orders could only be effective if they are confidential. Although I operate in a classified environment, my oversight role calls for me to be as transparent as possible with Canadians. I share my decisions with the National Security and Intelligence Review Agency, presided over by Ms. Deschamps, for post-facto review purposes. I publish redacted versions of my decisions on my office’s website. Decisions rendered under this bill would likewise be published.

My annual report, which was tabled in Parliament last Friday, also provides information on the impact of the activities that I oversee and on the significant legal issues at stake.

[*English*]

Would my office require additional resources for this new function? I have no control over the number of ministerial orders that I would review, nor how complex or voluminous each file might be. Another consideration is the potential effect of judicial reviews. These considerations could impact the resources my office needs. My role is on a part-time basis, and I adapt my work and my life accordingly. My expectation is that if my office requires additional funding, this will be provided in a timely manner. I would certainly appreciate a firm commitment from the minister to that effect.

One element I would raise for your consideration relates to the minister's extending, or not, the validity period of an order. Currently, there's no limit to the validity period or to the length of any extension. Under my existing jurisdiction, maximum validity periods are specified, and renewals require a new approval by the IC. I suggest a similar approach in this bill.

[*Translation*]

I will be happy to answer your questions.

The Vice-Chair (Frank Caputo): Thank you very much, Mr. Noël.

[*English*]

We are running a bit late, so I will propose, at least for this round, that we go to five minutes per round. I hope that's okay. I don't want anybody to lose their round.

With that, we will begin with Mr. Lloyd for five minutes.

Dane Lloyd: Thank you.

Thank you to the witnesses for being here.

Madame Deschamps, were you consulted in the drafting of this legislation?

Hon. Marie Deschamps: I understand that this question was posed to the minister.

I have been meeting with the minister, according to the statute, once a year. When we met in December for our yearly meeting, Bill C-22 did not come up.

Dane Lloyd: Philosophically, one reason Canada is such a great country is precisely because of the accountability we have—redundant levels of accountability. That's why I'm quite shocked that this is the second iteration of this legislation. We had Bill C-2 and now we have Bill C-22. The basic accountability things you talked about, like review capabilities, are not included. I'm highly frustrated given the seriousness of the issues this legislation seeks to address. It's things like child sexual exploitation, yet basic accountability measures like review are not being included.

Could you talk about the importance of why NSIRA should be involved in the review process?

Hon. Marie Deschamps: At NSIRA, we regularly receive information about authorizations, and we don't just ignore it. We integrate it into the bulk of our knowledge of the operations agencies are conducting. With that knowledge, we are building the amount of information we need to plan our activities and get to a better understanding of how agencies are operating.

It's very important that, specifically with this bill, we get the information as early as possible. That moment in time would be the minute the intelligence commissioner issues his approval.

● (1855)

Dane Lloyd: Thank you. I sincerely hope we can get amendments like the ones you proposed discussed here more fulsomely. I'm very frustrated that this wasn't included in the legislation by the Minister of Public Safety in the first place.

Ms. Curran, I brought this up with another witness. Does Meta advertise its privacy controls to its consumers?

Rachel Curran: We do, yes. We have a transparency centre that outlines all of our privacy policies. We implement, essentially, privacy by design into all of our products, and we make very clear to all users what these policies are.

Dane Lloyd: If you were to receive a secret ministerial order to install a device or create a capability so that law enforcement could circumvent those advertised privacy controls, how would you be able to tell your users that those things you're advertising are no longer allowable?

Rachel Curran: We wouldn't be, and this is a major issue.

I'm going to let my colleague Robyn get into this in more detail, because this is an important question.

Robyn Greene (Director, Privacy and Public Policy, Meta Platforms Inc.): Thank you so much for putting this question forward.

As drafted, the bill has a blanket secrecy provision that would essentially prevent us from being able to explain to our users that these changes were made and, if discovered, why they were made. This latter part is really important because, ultimately, our services are available around the world. This means there are security researchers, technical experts and journalists around the world who regularly decompile and reverse-engineer our products. Sometimes it's because they're trying to look for vulnerabilities and help us shore up our systems through bug bounty programs. Sometimes it's because they're trying to see if they can get any information on what our next product or feature releases will be. This happens with all companies like ours.

Ultimately, these kinds of changes will be discovered. It's not a question of “if”. As Rachel was saying, when it comes to the exploitation of a vulnerability, discoverability is a question of “when”. Providers would then be in a really significant conflict because users would completely lose trust in the security and privacy protections of our products.

Dane Lloyd: I'm sorry to cut you off, but I have limited time.

Apple threatened to leave the United Kingdom because of its laws. Do you foresee major companies also possibly having to leave Canada because of this legislation, if it goes unamended?

Robyn Greene: I can't speak to what other companies will do, but I think there are a number of companies that have gone on record, stating clearly that they're not open—

The Vice-Chair (Frank Caputo): Thank you very much. I'm sorry, but I do have to cut you off there.

Next, we have Mr. Zuberi for five minutes, please.

[*Translation*]

Sameer Zuberi: I thank the witnesses for being here.

[*English*]

I'm so happy to see you in front of us today. I have a lot of respect for the work that you have done throughout your careers.

I will start with you, Mr. Noël. Over the years, I have come across your work with respect to security certificates and many other pieces of national security legislation, and I have a lot of respect for this.

You stated earlier that one of your key functions involves privacy, looking at privacy with respect to this legislation. Would you suggest that it would be at all helpful for the Privacy Commissioner to be involved in this legislation and this process?

Hon. Simon Noël: Not knowing exactly what is in the privacy law, I think he is already following the work I'm doing—through his personnel. I think he would be doing the same if it was the case. The distinction to be made between the Privacy Commissioner and me is this: I'm involved in the decision-making process; the Privacy Commissioner is not involved in any government decision.

Sameer Zuberi: I understand.

Currently, Canadians have a reasonable expectation of privacy. This legislation will shift that landscape. Can you explain how it would shift that landscape?

Can Canadians still expect to have a reasonable expectation of privacy, given the scope of this legislation?

● (1900)

Hon. Simon Noël: It's hard to guess what will be in the future. With the new era we're in, gone are the days of the telephone book that police organizations could go and consult. The Meta groups and the others control all of that information. The government is put in a position of trying to improve the system of investigation across Canada.

[*Translation*]

He is trying to establish a framework, an architecture to be able to do so.

[*English*]

I would suggest to you, sir, that Canadians, when they hear about pedophile issues and bank fraud, expect the system to adapt to the new era. Measures have to be undertaken. This is one proposal. Some people don't like part 2, but somebody at some point will have to decide how the data banks, essential to police organizations, will be used, and that's one example.

Sameer Zuberi: I know you've spoken about the duty of candour of CSIS and other agencies. I understand your current role is different from your role in the past, but, Madam Deschamps or Mr. Noël, if you have any comments about potential concerns around duty of candour or compliance by policing organizations and those that have the authorities.... Do you foresee any potential concerns?

Hon. Simon Noël: My past experience, as you have noted, has shown that I've had to call it as it is: a breach of duty of candour. In my present position, I have put the burden on both agencies to tell me, to brief me, on everything that they're going to present to me. If they don't tell me exactly what I should know or not know, they will pay for it, because a decision will not be granted.

Sameer Zuberi: I'll use the remainder of my time to plead to Meta that it please curate an environment online that is family-friendly—to be honest, not just one that is family-friendly but one that invites people to positively participate. As elected officials, we have so many comments on our social media that do not create environments that encourage positive discussion.

I just want to put that out there to you. Thank you.

The Vice-Chair (Frank Caputo): Thank you, Mr. Zuberi. You are out of time.

[*Translation*]

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

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

I'm very glad to hear from you, Ms. Deschamps and Mr. Noël. I think you are the only francophones to have spoken in the four hours since the meeting began. So, that's music to my ears. I wanted to tell you that.

Ms. Deschamps, it's fair to say that the National Security and Intelligence Review Agency is a young organization. I think it's been around for about six years. I feel like I'm the member encouraging my colleagues to learn more about the agency, because it's still pretty unknown. By attending your briefings, I've come to realize just how important it is in terms of protection and oversight.

Regarding Bill C-22, the minister does not seem to understand what you are asking for and what I am about to ask for, namely that the agency be notified. This is not a request for you to be involved in the decision-making process. We know that, under the bill, this is the job of the intelligence commissioner.

Could you explain to us why, in Australia or other countries, they have chosen to allow agencies equivalent to yours to provide superior protection and surveillance by granting them access to real-time information?

Hon. Marie Deschamps: Thank you for clarifying that. While listening to some of the testimony, I got the impression that there was some confusion regarding the respective roles of the agency and the office of the intelligence commissioner.

The intelligence commissioner grants prior authorization to carry out activities, and subsequently, the agencies proceed with their activities. We examine, for example, the governance of these agencies. Primarily, what we examine is the legality and reasonableness of their activities and whether they use their powers only when necessary. So, we examine the activities after they have been carried out by—

● (1905)

Claude DeBellefeuille: Ms. Deschamps, I'm sorry to interrupt you, but, as you know, I only have five minutes.

We understood that perfectly well when you gave your speech. What I want to understand, and what I want you to explain to people, is the fact that some countries have made a different choice than the one the government made in Bill C-22. These countries notify their oversight body in real time of decisions made, for example, by an intelligence commissioner.

Canadians and Quebeckers would benefit from knowing that the agency is informed in real time, as this would reassure them. If the agency is informed a year after the fact, it requires a significant investigative effort. Furthermore, it does not necessarily have a large team that would allow it to quickly determine if the actions taken were not in compliance with the rules.

Did I understand that correctly?

Hon. Marie Deschamps: That is exactly right.

For example, in Australia, the turnaround time is only a few days. This saves the agencies that oversee intelligence activities from having to request information.

When you are forced to request information, it is not efficient for anyone. You have to do it on a case-by-case basis, with each of the agencies involved. It takes time for the body requesting the information, and it takes time for the agencies receiving the request. So, all we're looking for is greater efficiency. If we receive the information automatically, it avoids this entire process.

Claude DeBellefeuille: During his testimony, the minister said that if such an amendment were proposed, he might disagree somewhat. From what I understand, he feels that it would slow down the process. However, I believe that would not be the case, because the bulk of the work is done by the intelligence commissioner, who has a significant responsibility.

However, if you are there, aware of the situation, and keeping track of what is happening, it will allow you to be more effective and quicker in detecting non-compliant activities.

It seems obvious to me, Ms. Deschamps, that citizens and businesses are currently concerned. The agency would serve as an additional safeguard. Why not take advantage of it?

Hon. Marie Deschamps: The agency would likely be there, but things are changing so quickly, especially in terms of technology.

So, we would be there at a time when the information might be outdated. What we want is efficiency. We want to spare all teams from having to go out and find information, and we want to be able to prepare more effectively when it comes to reviewing the activities that have been carried out.

We want to be better prepared and in a better position to review them.

Claude DeBellefeuille: The idea is that the government draws inspiration from the Five Eyes, but it has not always adopted their best practices. In fact, it seems to me that Australia has better practices when it comes to oversight.

Isn't that right?

Hon. Marie Deschamps: That is our view on this aspect, namely notification.

Frank Caputo: Thank you, Mrs. DeBellefeuille and Ms. Deschamps.

[*English*]

We'll now go on to Ms. Kirkland, whom I was supposed to recognize earlier.

I apologize for that. You have five minutes.

Rhonda Kirkland: That's all right. Thank you so much.

One of my colleagues on the other side used his last 30 seconds to implore Meta to limit free speech. I would like to use my first few seconds to implore Meta not to limit free speech. I will say that first.

Ms. Curran, you were rushed at the end of your testimony while finishing off. I want to give you half a minute to repeat your conclusion so we can really understand it.

Rachel Curran: Thank you, Ms. Kirkland.

We just have three asks—three recommendations for this bill. Remove obligations for companies to add government or third party surveillance tools or other software to their systems. That would include our company. Strengthen the definition of “systemic vulnerability” to explicitly rule out any requirement that would weaken or break encryption, mandate client-side scanning or otherwise introduce a security weakness. Codify the process for companies to challenge problematic requests. I think we heard that after-the-fact protections are really no protection at all. Those are our recommendations for dealing with part 2.

For what it's worth, we think part 1 responds to the criticisms that were made about part 14 of the previous bill, Bill C-2. It is a good framework, subject to a couple of tweaks, to provide law enforcement with the information it needs to conduct investigations. Part 2 is really the problem with this bill. We are recommending some pretty significant, fundamental changes to that part.

● (1910)

Rhonda Kirkland: Thank you very much.

I also want to give you a moment to respond to the intelligence commissioner's comments.

I understand we are in a new era. Things have changed in terms of what is available online and that sort of thing. The only thing you may want to comment on is this: Apparently, you control all this information, just like the phone book used to.

Would you like to comment on that at all?

Rachel Curran: Yes. I'll get my colleague Robyn to weigh in on that.

Rhonda Kirkland: Okay. Thank you.

Robyn Greene: Of course, we do not control all the information.

One thing that's critically important about the services we offer is this: People use our services for different things. That is why we are proud to be, really, the largest service provider of end-to-end encrypted communications services in the world. At the end of the day, people are extremely dependent on having secure and private mechanisms for communications, whether for friends and family, for running their business or for engaging in day-to-day life. The reality is that governments rely on end-to-end encryption, as well, to conduct government business and represent the interests of constituents.

The idea that technology is changing so quickly is one of the most important things for us to think about. Encryption is one technology that is changing very quickly but not in the way many people expect. One of the new waves of development in encryption technology is the implementation of post-quantum cryptography. One of the greatest threats we're facing over the course of the next several years is this: As we see advances in quantum computing, there need to be similar advances in post-quantum cryptography because that's the only type of cryptography that's going to be resistant to the ability to decrypt previously encrypted information.

One thing we're concerned about with this bill is that there are insufficient safeguards to ensure that encryption won't be undermined or that a mandate to break encryption won't be imposed. This will become significantly more dangerous in the future when you're looking at trying to build secure exceptional access—which is really a paradox in itself. It's not something that's possible to do. It will be much more difficult in a future state with post-quantum cryptography.

Rhonda Kirkland: There's so much to unpack here, and there isn't time to do it. I wish I could have you here for another hour.

I'll ask simple yes-or-no questions in this one.

I think you said this already. Would compliance with Bill C-22 introduce new systemic cybersecurity risks for global platforms operating in Canada, particularly when they are required to retain or produce metadata or subscriber information at scale?

Robyn Greene: As currently drafted, yes, it could.

Rhonda Kirkland: You said that vulnerabilities will be exploited. Is there anything at all in this bill that protects Canadians against this exploitation?

Robyn Greene: There's nothing sufficient. Right now, the provision around making sure that providers don't have to comply with an obligation that would introduce a systemic vulnerability does not offer sufficient process or enough scope and clarity of definition to be sure that we wouldn't literally have to introduce the systemic vulnerability that the bill is purporting to prevent.

Rhonda Kirkland: Thank you so much.

The Vice-Chair (Frank Caputo): Thank you very much.

Thank you, Ms. Kirkland.

Now, we go on to Mr. Housefather, please, for five minutes.

Anthony Housefather: Thank you, Mr. Chair.

I'll try not to geek out about a Supreme Court justice being here, but it's also something that's very exciting.

Roman Baber: Were you in law school?

Anthony Housefather: Yes, of course.

[*Translation*]

Ms. Deschamps, I believe you have already expressed your point very clearly. You sent a letter to the committee chair, Mr. Jean-Yves Duclos, on April 16, 2026. That letter contained two proposed amendments.

If these two amendments were adopted by the committee and, eventually, incorporated into the bill, would that be sufficient for you, with regard to the matters within your organization's purview?

● (1915)

Hon. Marie Deschamps: In a word, yes.

Anthony Housefather: All right. That's perfect.

Mr. Noël, thank you very much for being here.

You mentioned the need for additional resources. That's for sure. The bill provides for a very significant mandate for you.

Are there any changes we should make? If you tell me that's not your role, I'll understand.

However, do you have any suggestions for improving the bill, aside from increasing your resources?

Hon. Simon Noël: The only thing I recommend is to specify, in subsection 7(3) of the bill, in part 2, that the decision to issue an order against an electronic service provider must be made based on a standard of reasonableness and proportionality.

To explain very briefly, paragraph 7(3)(a) must be balanced against the issue of the “potential impact of the order on the persons to whom the electronic service provider provides services”, in paragraph 7(3)(d), and with the issue of the “potential impact of the order on privacy protection and cybersecurity,” in paragraph 7(3)(e).

There must be a balance between these elements. That is why I am talking about reasonableness and proportionality.

Anthony Housefather: Could you please submit your proposed amendment in writing to the committee?

Hon. Simon Noël: Yes.

Anthony Housefather: Thank you very much.

[*English*]

Now let me come to Meta. Thank you, by the way, for coming all the way from D.C. It's very much appreciated.

Rachel, I know you didn't come from quite as far, but thank you also for being here.

I don't think it's feasible that we're just going to drop part 2, but I do understand the requirement. One thing that I'm very sympathetic to is the question of clarity—first of all, a clear definition of a systemic vulnerability; and second, a clarity that the order, should a section order be given, is still subject to...that an order can't require you to do something that creates a systemic vulnerability.

Would that largely assuage some of the concerns that you have?

Rachel Curran: If you clearly defined protection of encryption in the bill, that would go a long way.

Anthony Housefather: That nobody is going to ask for an end-to-end encryption to be broken...?

Rachel Curran: Exactly, and I know that the government has said that their intent is not to break or weaken encryption. If that's the case, make it clear in the bill.

Also, if you included in the bill a provision that prevented the government from making a request that it reasonably believed would create a systemic vulnerability.... Right now, the onus is all on companies. It's all on us to challenge a request and say that it will create a systemic vulnerability, and the process for doing that is not entirely clear. If there were some onus on the government not to make requests that it believed would create a systemic vulnerability, that would also go a long way towards assuaging these concerns.

Anthony Housefather: Thank you.

I wanted to also note that, of course, a lot has come up about the terms and conditions of Meta. I would say that, having read the extremely long terms and conditions, it would be very easy to put in a caveat to say that one of the many exceptions to the privacy that you're guaranteeing to the user would be that Canadian law should, in the event that X and X happened....

Let me just come back. Since we have an expert from the States, can you just talk to us about the major differences between the two major pieces of U.S. law and this one, and where you see the distinctions?

Robyn Greene: Under U.S. law, the Communications Assistance for Law Enforcement Act is the governing authority, where specifically telecommunications providers and ISPs are subject to obligations to make sure that their services can be intercepted, essentially, in response to wiretap act warrants.

There are very clear exceptions for over-the-top services, such as the services Meta offers and other apps. We are not subject to the same requirements. In addition to that, there are protections for encryption explicitly in that law. The All Writs Act is also not really a clear path and has never been established in court as a mechanism for successfully mandating an encryption back door.

The last point I would make is that it was the very provisions of CALEA that led to the vulnerabilities that resulted in the Salt Typhoon and Volt Typhoon attacks.

The Vice-Chair (Frank Caputo): Thank you very much, Mr. Housefather.

[*Translation*]

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

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

Commissioner, in another legislative context, you have developed a practice of working closely with or collaborating with the National Security and Intelligence Review Agency. This is already your practice.

Isn't that right?

● (1920)

Hon. Simon Noël: Yes.

Claude DeBellefeuille: Your two offices work together.

Hon. Simon Noël: We work in a complementary manner.

Claude DeBellefeuille: If the government were to accept the proposed amendments, it would not be an additional burden for you. It would simply be a continuation of a practice you already use in other contexts.

Is that correct?

Hon. Simon Noël: There would not be any additional work. When we render our decisions, Mrs. DeBellefeuille, they are automatically forwarded to Ms. Deschamps's office.

Claude DeBellefeuille: All right. So that work is already done.

Hon. Simon Noël: I don't want to speak for Ms. Deschamps, but this is just about the decision. There is a whole other set of documentation that needs to follow, which delays the work a bit. We have no control over that.

Claude DeBellefeuille: I understand.

I've seen the highlights of your latest report, Mr. Noël. You've issued 14 decisions over the past year. That's a record year. I asked the staff if they had assessed your new role with you in terms of workload and intensity. In response to my question, they told me that you've discussed it and that it should be fine. However, you said right off the bat that it's a bit of a leap into the unknown. You'll have to adapt a little.

Does your experience give you an idea of what to expect in terms of pressure and intensity for your office?

Hon. Simon Noël: It is difficult to predict exactly how—

Claude DeBellefeuille: I do apologize, but I can't hear you.

[*English*]

The Vice-Chair (Frank Caputo): Madame DeBellefeuille has the floor. I'm pausing the time here.

Go ahead, Madame DeBellefeuille.

Thank you.

[*Translation*]

Hon. Simon Noël: I work part-time.

Claude DeBellefeuille: You work part-time. What does that mean?

Hon. Simon Noël: I will explain it to you. That is precisely the point I want to raise.

If I compare my job to that of a judge, who is 100% occupied with it, my work currently occupies me 40% or 42% of the time. There is still some leeway. There is still room. I don't see a problem, except that we would like to have a commitment once we see how the matter unfolds.

Claude DeBellefeuille: You want it to be easy to obtain.

Right?

Hon. Simon Noël: That's exactly it. We don't want to be forced to go begging.

Claude DeBellefeuille: You don't want to be forced to ask Mr. Sabia to give you a little more.

Is that correct?

Hon. Simon Noël: Exactly. We don't want to say to them: “Please, give us this.” I have my independence, and I intend to preserve it. I won't go begging. Perhaps there will be other ways to apply pressure at that point, such as delaying a decision they'll want to get quickly.

Claude DeBellefeuille: You have the upper hand.

Frank Caputo: Thank you for your comments, Mr. Noël.

[*English*]

Now, we go to Mr. Baber for five minutes, please.

Roman Baber: Thank you very much, Chair.

Welcome, Justice Noël.

Madame Deschamps, like my colleagues, I started law school the same year you were appointed a Supreme Court justice. It's truly an honour to have you appear before our committee.

Justice Noël, I understand the function of the of intelligence commissioner is to essentially approve or not approve certain intelligence and other security activities. Is that correct?

Hon. Simon Noël: Yes.

Roman Baber: I've also heard some of your remarks earlier to my colleagues. Have you had a chance to review the bill?

Hon. Simon Noël: I glanced at it. I looked more precisely at my role and what was expected.

Roman Baber: Do you understand that you will be expected to sign off on orders made by the Minister of Public Safety to essentially install surveillance systems on private businesses? Do you understand that?

Hon. Simon Noël: I fully understand. It's not something new to me. I'm aware of lots of things—

Roman Baber: I appreciate that.

Hon. Simon Noël: —that I cannot define.

Roman Baber: What is important to me at this stage is who might be subject to that.

I asked the clerk to give you a copy of the bill.

Hon. Simon Noël: Yes, I got it.

Roman Baber: Please look at page 37. I'll take you there very quickly.

Hon. Simon Noël: Yes.

Roman Baber: I'm at page 37, on the top left. It says, “electronic service provider” means a person that, individually or as part of a group, provides an electronic service in Canada or carries out part of its business in Canada.

Then the question becomes what an electronic service is, and that is at the prior page. If you go to the earlier page, it says, “electronic service” means a service, or a feature of a service, that involves the creation, recording, storage, processing, transmission, reception or making available information in electronic form or other technological means.

That sounds to me like a law firm that has a server that runs emails of its clients. It sounds to me like a bank. It sounds to me like a doctor's office.

● (1925)

Hon. Simon Noël: Solicitor-client....

Roman Baber: It's beyond solicitor-client. It could be your local bakery shop.

Hon. Simon Noël: Okay.

Roman Baber: My question to you is this: Do you believe that the intelligence commissioner, in your capacity, should be able to make mandatory orders to plant government-demanded technological devices to spy on customers of everyday Canadian businesses without a court order?

Hon. Simon Noël: If I look at what the minister has to provide to me, it's listed in proposed subsection 7(3). If I have an issue such as the one that you're raising, the bakery shop, it will raise in my mind major questions. I'm just saying that without knowing exactly what would be done, I don't know in the end what I could do.

I would like you to know that in the job that I have presently in my first year, I had situations I never thought I would face and—

Roman Baber: I appreciate that.

If I may, I only have about a minute left.

Hon. Simon Noël: No, I don't want to use your time. Go ahead.

Roman Baber: In fairness to my friends, my Liberal friends disagree as to how we interpret the statute. They believe that it only applies to Internet service providers. I don't read the statute that way, but I think I should afford them that fairness.

I'm curious. I'm not going to ask you how many times over the number of years you've been asked to approve or disapprove an order, but without breaching any confidentiality, are you able to tell me what the ratio of success is of the government when they show up?

Hon. Simon Noël: Yes, I could tell you that I—

Roman Baber: Is it fifty-fifty...sixty-forty?

Hon. Simon Noël: I'll just give you a big picture. Madame De-Bellefeuille talked about 14 decisions that I rendered last year. I think they're going to come down to approximately nine this year. I must have signed close to 50 decisions since I began doing that and, out of that, I would say around 15% of activities were denied.

Roman Baber: Is that one-five?

Hon. Simon Noël: It's one-five, 15%.

Roman Baber: Then for 85%, the government got their request.

Hon. Simon Noël: Yes. Not the government...it was CSE and also Public Safety.

Roman Baber: I didn't expect that, but I appreciate your candour.

Moving on to Meta—

The Vice-Chair (Frank Caputo): Thank you very much, Mr. Baber. Unfortunately, we're over time.

[*Translation*]

The last member to speak tonight is Mr. Ramsay.

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

[*English*]

Jacques Ramsay: I have a question for Meta.

I understand you said that as the law is right now, you wouldn't be able to protect the privacy of Canadians. Are you actually acknowledging that if the law passes, Canadians should close their Facebook and Instagram accounts?

Robyn Greene: I don't think we're suggesting that. I think the concern is that if the law passed, it creates an authority for the government to serve orders on us that could fundamentally break the security guarantees of our company or those of any other subject service provider.

Jacques Ramsay: Having heard what you just heard, which is that the intelligence commissioner will validate the order of the minister and then you have a judicial review that you can apply for so that this will go to court, do you still have the same fear?

Robyn Greene: When we're looking at the legislation, we are hoping for a certain level of legal certainty, not only for ourselves and our ability to conduct our business operations but also for our users to—

Jacques Ramsay: I hear you, but I disagree. I think there's a fair amount—

A voice: It wouldn't matter if—

Jacques Ramsay: I'm sorry—

The Vice-Chair (Frank Caputo): Just a minute, Mr. Ramsay.

It's very difficult for the interpreters, as somebody who has once or twice interrupted a witness, I've been told that—but it was only the ministers.

Let's start again.

[*Translation*]

Please continue, Mr. Ramsay.

[*English*]

Ask your question of the witness, please.

Jacques Ramsay: The fear for Meta is, as they said, that there would be spyware, somehow.

● (1930)

[*Translation*]

Mr. Noël, if the minister issued an order to install spyware, could you issue an opinion against that?

Meta seems to fear that the minister might abuse his powers.

Hon. Simon Noël: I can assure you that this would be a very important factor and that I would look into it seriously.

[*English*]

I would like to reassure Meta that in that case, you would present to me a document. If it's convincing, I would certainly look at it seriously and make up my mind down the road.

I do know what encryption is all about. I know how important it is. If something is trying to circumvent the encryption and open up the channels to other things, I still have common sense. I know what I'm doing. My intent, at the end, is to protect the privacy of Canadians, wherever they are.

[*Translation*]

Jacques Ramsay: Mr. Chair, I have nothing further to add. I will yield the remainder of my speaking time to Ms. Acan.

[*English*]

The Vice-Chair (Frank Caputo): It looks like we have another lawyer here.

Voices: Oh, oh!

The Vice-Chair (Frank Caputo): You have two minutes and 15 seconds.

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

Ms. Greene, Meta already complies with the U.S. CLOUD Act, which gives, as you mentioned, American authorities the power to compel U.S.-based technology companies to produce data under their possession, custody or control, regardless of whether the data is stored in the U.S., Canada or elsewhere abroad. Under the CLOUD Act, the U.S. authorities can obtain access to Canadians' data, through judicial orders served on companies like Meta, and Meta accepts those obligations as a part of operating in the United States.

Bill C-22, similarly, requires lawful access based on Canadian legal authorization—

The Vice-Chair (Frank Caputo): Could you slow down just a shade, please, Ms. Acan, for the interpreters?

Sima Acan: I'm sorry.

Bill C-22, similarly, requires lawful access based on Canadian legal authorization and judicial oversight, yet Meta has raised significant concerns about Canada's proposal. Can you explain why Meta considers it acceptable for U.S. authorities to compel access to data globally under the CLOUD Act, but objects when Canada seeks to ensure its own—

Roman Baber: I have a point of order.

I think it's very important that if my colleague opposite is going to put a fact on which she is going to predicate an argument to the witness—

Sima Acan: It's not an argument. It's a fact.

The Vice-Chair (Frank Caputo): Okay, let's just let him—

Roman Baber: Excuse me. Let me finish my point of order.

It has to be truthful and accurate. In one case, it's a judicial authorization. In this case, it's without judicial authorization. That's the difference.

The Vice-Chair (Frank Caputo): This may be—

Sima Acan: There is still authorization here.

The Vice-Chair (Frank Caputo): We were doing so well.

We're near the end of the night. I know that different people can disagree on different points and on what they read into things. I take your point, Mr. Baber. I have known Ms. Acan to always attempt to be on the up and up, so this may just be—

Anthony Housefather: I have a point of order, Mr. Chair.

I'm sorry. That was not a point of order. You know that very well. The witness is perfectly capable of responding in that way if that is what the witness feels—please.

Roman Baber: Is there a point of order in that point of order?

The Vice-Chair (Frank Caputo): Okay, we are now past.... We are well into debate here.

Ms. Acan, could you please ask your question again?

Sima Acan: Thank you very much.

I brought up the CLOUD Act because there are two acts here, which have the same purposes, and in our act we do have some orders too.

My time is still there. Is that not right?

The Vice-Chair (Frank Caputo): Yes, you have one minute left.

Sima Acan: Okay.

Can you explain why Meta considers it acceptable for the U.S. authorities to compel access to data globally under the CLOUD Act, but objects when Canada seeks to ensure its own law enforcement agencies can lawfully access information, under Canadian law, to investigate child exploitation, human trafficking, organized crime and terrorism? Why should Canadians accept a situation in which U.S. authorities can lawfully access our data, through Meta, but Canadian law enforcement face additional barriers?

The Vice-Chair (Frank Caputo): Again, Ms. Acan, you need to slow down.

Sima Acan: That was my question. Thank you.

The Vice-Chair (Frank Caputo): You have 20 seconds for an answer.

Robyn Greene: My very short answer is that the CLOUD Act does not provide for what you're describing, and U.S. law does not have any provision that would allow the U.S. government, with or without a court order, to mandate providers to build an encryption back door or otherwise put government surveillance software onto their systems. That is the primary point of concern with part 2.

The CLOUD Act would allow for increased access to communications data under part 1, and we are supportive, with some amendments, of part 1 moving forward. We would certainly love for Canada to enter a CLOUD Act agreement.

● (1935)

The Vice-Chair (Frank Caputo): We will look forward to those amendments.

I know that this has been a very long four hours.

[*Translation*]

I would like to thank the interpreters, the analysts, the clerk and the members.

[*English*]

Thank you very much. Have a great night.