HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

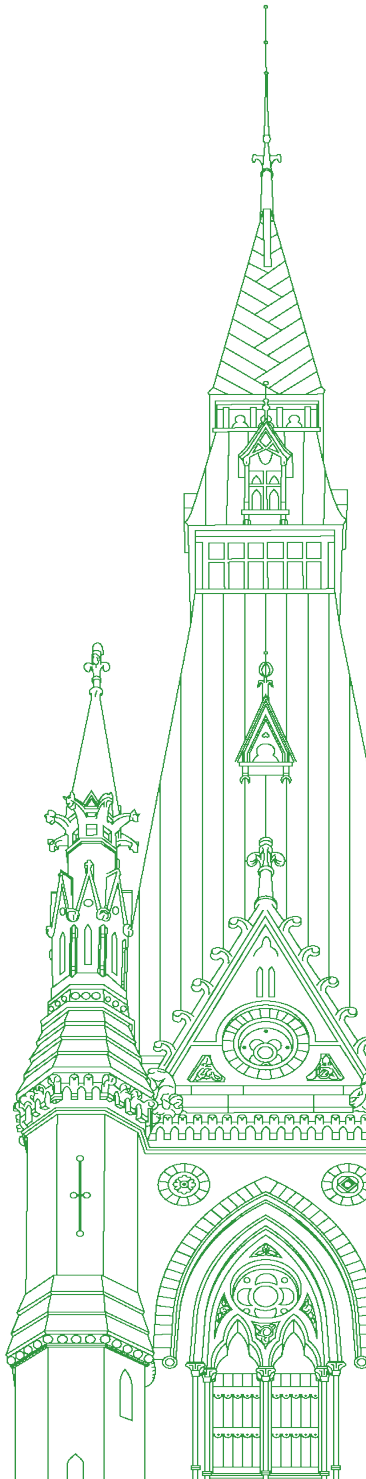
44th PARLIAMENT, 1st SESSION

Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 031

Monday, August 8, 2022



Chair: Mr. Pat Kelly

Standing Committee on Access to Information, Privacy and Ethics

Monday, August 8, 2022

● (1505)

[*English*]

The Chair (Mr. Pat Kelly (Calgary Rocky Ridge, CPC)): I call this meeting to order.

With that, we'll ask the photographers with cameras to leave the room.

Welcome, everyone, to meeting number 31 of the Standing Committee on Access to Information, Privacy and Ethics. Pursuant to Standing Order 108(3) and the motion adopted by the committee on Tuesday, July 26, 2022, the committee is meeting to study device investigation tools used by the Royal Canadian Mounted Police.

Today's meeting is taking place in a hybrid format pursuant to the House order of Thursday, June 23, 2022.

For the first hour of this meeting, we are pleased to have the Honourable Marco Mendicino, privy councillor, member of Parliament and Minister of Public Safety.

With that, I will invite the minister, if he is ready, to proceed with opening remarks.

Minister, do you have your proper headset with you?

The Honourable Marco Mendicino (Minister of Public Safety): I am in the regional office in Quebec here, and I'm told that these are devices that have been approved by PCO. If there is any trouble, please let me know.

The Chair: I'll make a quick survey of the room and the interpreters to confirm that we have good audio. Are we okay with the minister's audio?

I'm not seeing any objection, and I didn't see any reaction from interpretation. I see some nodding, okay.

With that, thank you, Minister. Go ahead for up to—

Ms. Iqra Khalid (Mississauga—Erin Mills, Lib.): I have a point of order, Mr. Chair.

The Chair: I'm sorry; there seems to be a point of order before we begin.

Ms. Khalid, you have a point of order.

Ms. Iqra Khalid: Yes, Chair, I want to review something from the last meeting. Near the end of the meeting, the committee decided to continue for another round of questions, and, at the request of an opposition member, Chair, you changed the timing for that additional round to be five minutes for each questioner as opposed to what was outlined in the routine motions.

I would like to point you to one of the routine motions that was passed unanimously by this committee on December 13, 2021. On motion of member Lisa Hepfner, it was agreed:

> That witnesses be given five minutes for their opening statement; that whenever possible, witnesses provide the committee with their opening statement 72 hours in advance; that at the discretion of the Chair, during the questioning of witnesses, there be allocated six minutes for the first questioner of each party as follows: Conservative Party, Liberal Party, Bloc Québécois, New Democratic Party. For the second and subsequent rounds, the order and time for questioning be as follows: Conservative Party, five minutes; Liberal Party, five minutes; Bloc Québécois, two and a half minutes—

The Chair: If I may, Ms. Khalid, I am fully aware of the motion and its content. If you will recall, in the meeting, when there was a request from one member to have a five-minute round when we had exhausted three full rounds, there appeared to me to be unanimous consent to proceed in the way that I did. I was merely allowing members, with the time we had left after a lengthy meeting, to go ahead, and I gave each party five more minutes.

If I may infer from this intervention that you will not agree subsequently to any other deviation from that motion, then that is noted. I don't think we're going to have time for that to be relevant, anyway, with any of our further meetings, given how tight they are.

If that's sufficient, may I proceed with our witness?

Ms. Iqra Khalid: Yes, thank you.

Mr. Matthew Green (Hamilton Centre, NDP): This is a point of order, Mr. Chair.

The Chair: I'm sorry; we have another point of order.

Go ahead, Mr. Green.

Mr. Matthew Green: Referencing the Standing Orders and the routine procedures, has the minister provided this committee with his opening remarks in advance of the committee?

The Chair: I did not receive any. I'll ask the clerk if any were received.

Okay, the clerk has, in fact, received remarks, but it does appear that they were not distributed to members. I did not receive them, so we will try to get those out as quickly as possible.

Thank you, Mr. Green.

With that—

All right, we're burning up the time that we have with the minister, but go ahead.

[*Translation*]

Mr. René Villemure (Trois-Rivières, BQ): We can't see the minister, Mr. Chair.

Hon. Marco Mendicino: May I begin, Mr. Chair?

[*English*]

The Chair: We're sorting out technical...

Hon. Marco Mendicino: That's no problem.

The Chair: I think this is a little better now. I understand the problem we had, but I think it's been resolved.

With that, go ahead, Minister. You have the floor.

Hon. Marco Mendicino: Thank you very much, Mr. Chair and colleagues.

I want to begin by thanking all the members of the committee for the study on the intersection of technology and policing, including the recent reports on facial recognition technology. I welcome the opportunity to talk about the adoption of new tools and technologies, especially as they concern transparency, privacy and legal and ethical standards.

Technology and policing have always been closely interconnected, but today's tech is advancing exponentially.

● (1510)

[*Translation*]

This progression extends from the evolution of mobile and wireless, to supercomputing, advanced analytics, biometrics, surveillance, forensics and beyond.

It's imperative that law enforcement bodies keep up with the pace of change. It's crucial that we do so to pursue those who would exploit new technologies for malicious intent.

This is necessary not only to increase efficiency, but also to closely examine how law enforcement selects and implements these technologies, to ensure the privacy, rights and freedoms of Canadians. In so doing, we must get that balance right.

[*English*]

For my part today, colleagues, I am pleased to provide a brief overview of the tools used by the RCMP.

The RCMP uses investigative technology and cutting-edge scientific tools in the areas of forensic science, fingerprinting, biometric and DNA data and surveillance, among other areas. Forensic science and identification services, for example, are integral parts of national police services, often relying on advanced science and technology.

Through these services, groundbreaking technology helps to identify biological evidence collected from crime scenes, examines firearms, seized materials and suspect counterfeit currency or I.D., and screens for a broad range of drugs and poisons and helps to provide expert scientific testimony in courts.

With respect to investigative technology specifically, the latest technology available to the RCMP helps to link crimes together, secures records and documents at crime scenes, identifies suspects and victims writ large and helps to keep Canadians and our communities safe.

The RCMP's CAIT program, or covert access and intercept team, uses approved technology to collect data that cannot be collected using traditional wiretapping technology or other less intrusive investigative techniques. This is only used under judicial authorization for the most serious offences.

Further, their Special “I” program is primarily responsible for the lawful electronic surveillance mandate of the RCMP. This has been the unit responsible for all interception of private communications that can be obtained pursuant to authority under part VI of the Criminal Code. It involves technical installations and deployments of electronic surveillance equipment in support of policing investigations. It also involves monitoring and analysis of data and communications that have been lawfully intercepted.

[*Translation*]

But colleagues, through all these examples, I'll be clear that transparency and accountability, privacy, and respecting fundamental rights and the law are paramount. The Privacy Commissioner has echoed that sentiment. And the government is committed to making sure that is foundational to all activities, including training and operational processes.

In particular, one of the key outcomes of the commissioner's investigation and report on the use of facial recognition was the need for a centralized process for the adoption of new tools and technologies.

In March of last year, the RCMP created the national technologies onboarding program, or NTOP.

[*English*]

The purpose of the national technologies onboarding program, or NTOP, is to centralize, standardize and bring greater transparency to the processes that govern how the RCMP identifies, evaluates, tracks and approves the use of new technologies and investigative tools. It will be the first point of contact for any unit interested in using any new operational technology. It will also ensure that a thorough evaluation of the technology is completed, making sure that the technology meets all privacy, legal and ethical standards.

The NTOP has begun accepting new technologies for assessment and will continue to increase capacity as it moves towards becoming fully operational.

I want to highlight that the RCMP is fully engaged with the Privacy Commissioner's office to ensure that privacy impacts are assessed for all new uses of facial recognition being considered.

Legal considerations are equally taken into account for the use of technology at all stages, including through the Criminal Code, which sets out provisions for judicial authorization and requires that we report annually to Parliament on the use of electronic surveillance.

Given the RCMP's mandate and the necessity to safeguard the ability to effectively use on-device investigative tools, we are not always able to discuss all of the technical or operational details of these tools. Where that is the case, it is for operational integrity and security only.

I understand that I'm out of time. I will be happy to take any questions from members of the committee.

● (1515)

The Chair: Indeed you are, but I gave you a few seconds to finish. Thank you, Minister.

We'll go to Mr. Bezan for up to six minutes.

Mr. James Bezan (Selkirk—Interlake—Eastman, CPC): Thank you, Mr. Chair.

I want to thank Minister Mendicino for joining us today.

Minister, when did you first become aware that the RCMP was using on-device investigation tools like Pegasus?

Hon. Marco Mendicino: First, I want to be clear with members of the committee that the Pegasus technology is not used by the RCMP. That's the first thing I would clarify.

Mr. James Bezan: What technology are you using?

Hon. Marco Mendicino: Second, as I said towards the end of my remarks, Mr. Bezan, some of the investigative techniques are kept confidential to preserve operational integrity and ensure that we can bring people to justice when necessary. They are always consistent with the charter and privacy rights.

Mr. James Bezan: Have you issued guidelines that would provide better direction to the RCMP, CSIS and other federal agencies on how they use ODIT?

Hon. Marco Mendicino: Mr. Bezan, that's a good question.

There are stringent requirements in the Criminal Code that require accountability, including for what facts the RCMP will be relying on prior to the judicial authorization of this sort of technique. There are other safeguards that ensure only designated agents put those applications to the court. There is also the annual report that we file with Parliament. Of course, I invite any suggestions from this committee during your study.

Mr. James Bezan: Thank you.

Does CBSA, CSIS or other federal agencies that fall under your jurisdiction and authority use this technology, aside from the RCMP?

Hon. Marco Mendicino: Again, just to clarify, it's not Pegasus but we do use this technique.

Mr. James Bezan: How long has this technique been employed by Public Safety through its various agencies?

Hon. Marco Mendicino: To the best that I have been informed, the use of the technique commenced in or about 2017, but I would defer to the RCMP officials who are on the line if they wish to provide any additional details.

Mr. James Bezan: They're here in person and we'll get that from them later on in the committee hearing.

I know from my time in National Defence that the Minister of National Defence maintains the power to provide ministerial directive and authority in the event that warrants are not possible because of time of day or because it's the weekend or the middle of the night. Do you have the same authority and power, as public safety minister, to provide a ministerial directive to the RCMP to conduct surveillance on Canadians?

Hon. Marco Mendicino: I want to thank you for the question. It allows me to reiterate the importance of operational independence.

Elected officials do not conduct criminal investigations, nor are they are responsible for dispatching [*Inaudible—Editor*] the investigative techniques that are being—

Mr. James Bezan: As minister in charge of the direction of the agency, do you have the power to give ministerial authority when there is not the capability or opportunity—say, to prevent a national security threat that's imminent—to provide surveillance with a judicial warrant?

Hon. Marco Mendicino: Mr. Bezan, as you will know, it is the RCMP that applies for those powers, and they are authorized by the court, after a rigorous application, on the strength of a designated agent who submits an affidavit.

Mr. James Bezan: Minister, was this on-device investigative tool used while the Emergencies Act was invoked?

Hon. Marco Mendicino: To my knowledge it was not. Again, for further operational details, I would invite you to put those questions to law enforcement.

Mr. James Bezan: We'll raise that later.

As you know, National Defence was on training exercises on a King Air aircraft that was circling downtown Ottawa during protests. Were RCMP or CSIS officers on those planes when they were surveilling people who were on the ground for those so-called training exercises?

Hon. Marco Mendicino: Mr. Bezan, I would invite you to put any operational questions directly to law enforcement.

Mr. James Bezan: Have you been briefed on the RCMP's use of the remote activation of microphones and cameras on our mobile devices?

● (1520)

Hon. Marco Mendicino: I've had discussions with the RCMP and my officials. I've also had the chance to canvass the most recent annual report on the use of electronic surveillance, which was tabled for 2020. There's another report that is forthcoming for 2021. It is one of several mechanisms that we use to be open and transparent with the public about the use of this particular investigative technique.

Mr. James Bezan: As we know, Pegasus—although you're saying we don't use it here in Canada—has been deployed by state actors against politicians in other countries as well as journalists and human rights activists. We know that the U.S. has banned the use of Pegasus in the United States through the White House and actions by Congress.

How can you assure us that the software, the spyware that the RCMP and other government agencies are using, is not available to malign state actors here in Canada?

Hon. Marco Mendicino: Again, Mr. Bezan, I want to thank you for the question, and I can assure you that the question was put to our officials. The answer that I was given from them was that the branches within this portfolio do not use that technology. I would add in conclusion that there are rigorous protections that are put in place prior to the authorization of this particular technique, including applications that must go to a superior court judge on the strength of a designated agent who puts forth a thorough recitation of the facts on which the authorization is being sought.

The Chair: Thank you, Minister, and thank you, Mr. Bezan.

Now we'll go to Ms. Hepfner for up to six minutes.

Ms. Lisa Hepfner (Hamilton Mountain, Lib.): Thank you, Chair. Through you, I'd like to thank the minister for being here with us this afternoon.

Minister, in my former life as a journalist, I covered some terrorism trials. I could be wrong, but I understand that in your former life as a prosecutor you were involved in some terrorism cases, and based on the information provided to this committee by the RCMP, it looks like terrorism was one of the few crimes that the RCMP would use this technology to address.

I'm wondering if you can talk from your experience about why police might need to use this technology in the right circumstances with the right protocols and checks and balances in place.

Hon. Marco Mendicino: Thank you for the question, Ms. Hepfner. It's not often that I get to compare notes on prior professions in the kind of alignment in which you just posed it, your being a former journalist and I being a former federal prosecutor.

Yes, I am familiar with the rigorous steps that have to be followed in order to deploy this kind of electronic surveillance technique. It is not an easy thing to obtain. There are numerous steps that have to be followed, as I pointed out in my prior answers to Mr. Bezan.

First and foremost, there needs to be an application submitted to a superior court judge. That judge then has to take a look at the facts in very meticulous detail, which will offer some evidence or information of a very specific offence that is being breached. I would point out that, as I think is implied in your question, you can't apply for this type of investigative tool or indeed wiretaps generally for any old criminal offence. There are a limited number of very serious offences that are listed under part VI of the Criminal Code for which this technique would be eligible.

After that, the judge has to engage in a balancing exercise to determine, among other things, whether the interception, the technique, is necessary and whether it's pressing and urgent enough that it requires the technique to be afforded to the state for the purposes of acquiring information that could then be potentially used as evidence in a subsequent criminal proceeding.

Again, there is a lot of attention to detail. It is not uncommon for the courts to put questions back to designated agents before approving these judicial authorizations, precisely because we place paramount value on the protection of people's privacy, individual privacy rights and other protections under the charter.

There is a lot of protection built in to the Criminal Code, precisely to strike the balance of ensuring that the state has the tools that are necessary to protect the security and safety of all Canadians while at the same time upholding people's charter rights.

● (1525)

Ms. Lisa Hepfner: I think you mentioned that a judge would not approve these warrants if there were another way for police to collect this information. It's only a last resort.

Hon. Marco Mendicino: That's correct. It's typically referred to as investigative necessity. What the state has to demonstrate—what law enforcement has to demonstrate—is that there were efforts to exhaust other techniques prior to coming to court with a request for a judicial authorization under part VI, including some of the techniques that are the subject of the study before this committee. It really is seen as not a first resort, nor a tool of convenience. Rather, it's a tool of investigative necessity to demonstrate restraint, because it is important that we protect people's privacy.

Ms. Lisa Hepfner: There seems to be a lot of concern about mass surveillance. How do we know whether or not this occurred? How can we ensure that mass surveillance, which is not allowed, as you mentioned, is [*Technical difficulty—Editor*]?

Hon. Marco Mendicino: I think that's a very important question. Certainly, my hope is that through your study and through the contributions of all members of this committee, we can enhance openness and transparency about how law enforcement deploys these techniques.

I would say the central challenge right now for all state actors who are in the business of protecting Canadians is that they are confronted increasingly with complex encryption, which is intended to subvert law enforcement and subvert detection. The risks and consequences that flow from highly sophisticated encryption technology are that people can get away with crime and can undermine the health and safety of all Canadians.

Again, some of the techniques being deployed are intended to really frustrate the efforts of sophisticated criminal organizations and other bad actors, whether they be state or non-state, for the purpose of protecting Canadians. That's really going to be advanced by the work you are doing in studying and shining a light on these techniques, as well as by the annual reports that are filed on the use of electronic surveillance. Again, I invite the committee to look at that report and make suggestions on how we can continue to improve it if necessary. There is also the ongoing work that law enforcement does with NSICOP and NSIRA. All of these branches together cumulatively contribute to transparency and openness about how we are using these techniques—again, quite sparingly and as a last resort—to protect the health and safety of Canadians.

Ms. Lisa Hepfner: Thank you.

I think that's my time, Chair.

The Chair: Yes, that's about right, so thank you.

[*Translation*]

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

Mr. René Villemure: Thank you very much, Mr. Chair.

Mr. Minister, thank you very much for being with us today.

We're talking about a matter of trust. I'm wondering what we are to think about the revelations made by La Presse and web-based media Politico.

What effect do these revelations have on people's trust in the department or the RCMP?

You tell us that the RCMP is fully committed to the Privacy Commissioner, but this morning, the Privacy Commissioner seemed to be telling us that this agency was not that committed.

What is the cumulative effect of this on the public?

Hon. Marco Mendicino: Thank you for the question.

I completely agree with you that trust is one of the keys to openness and transparency.

I thank the committee for undertaking this study. It will give us the opportunity to study the technologies and techniques used by police forces, including the RCMP.

As I mentioned earlier, Mr. Villemure, there are a lot of challenges on the ground right now, in a geopolitical context where criminal organizations are using encryption to thwart police efforts.

So this study is an important opportunity to increase transparency and determine how the RCMP uses these techniques. It will help build trust.

Mr. René Villemure: It's a fact that technology is changing rapidly. We have to try to set limits on something that is not.

Hon. Marco Mendicino: You're absolutely right.

Mr. René Villemure: During your opening remarks, you mentioned that the RCMP was doing an assessment to see if the tool was too intrusive.

You were careful not to name the tool. However, this self-evaluation of relevance is not very transparent. I get the impression that the RCMP is assessing itself. I come back to the issue of trust, because I doubt the transparency of this assessment.

What is your observation on this?

● (1530)

Hon. Marco Mendicino: That's a good question.

The Criminal Code process for obtaining a wiretap authorization includes criteria that must be met. You have to demonstrate very rigorously to a superior court judge that the criteria are met. One of the obligations of the police and the RCMP is to show the judge that there is no other option and that all options to move the investigation forward have been exhausted. This is an example of a safeguard that is in place.

In addition, there are mechanisms in place, including the annual report to Parliament. This report refers to the date on which the authorization was granted by the superior court.

I invite all members of this committee to offer further suggestions for strengthening transparency mechanisms, because this will help build trust. We need to maintain trust everywhere so that we can use this tool in a way that respects the charter and all the rights it provides.

Mr. René Villemure: Would it be appropriate to bring in a third party to help the process to ensure that there is a healthy distance and to prevent the RCMP from assessing itself?

Hon. Marco Mendicino: I think so, yes.

There are already third parties, including the Privacy Commissioner, the National Security and Intelligence Review Agency, and the National Security and Intelligence Committee of Parliamentarians.

Many agencies have the power and authority to review information, which is traditionally protected by national security legislation and other privileges. It allows us to further increase trust. Third parties are already there to help us do this work.

Mr. René Villemure: Thank you very much.

Do you believe that judges who issue warrants as requested by the police have the technical ability to assess all of these tools?

These are still complicated things.

Hon. Marco Mendicino: That's an excellent question.

The answer is yes, judges are absolutely competent.

Judges have a good understanding of the statutory criteria. They know how to balance the government's duty to protect everyone with respect for all charter rights.

Judges have the expertise, experience and competence to do this, to seek balance. That's why I have confidence in this process. Institutions exist to protect all the rights of Canadians.

Mr. René Villemure: Even though it is done carefully, third parties are there to monitor the process, and there is some accountability, we can still conclude that the RCMP is spying on Canadian citizens.

Is this correct?

Hon. Marco Mendicino: Yes, this is precisely the RCMP's job. Officials and those responsible are there to answer technical and operational questions, to tell you how these techniques are used in the field in the context of investigations.

However, that doesn't mean that there's no room for improvement. That's why I encourage the work that this committee is doing. I invite committee members to offer suggestions and recommendations to strengthen how these tools are used by police forces, including the RCMP.

Mr. René Villemure: Rest assured, that's our goal as well.

Thank you.

Hon. Marco Mendicino: Okay.

Thank you.

[*English*]

The Chair: Thank you.

We now have Mr. Green for up to six minutes.

Mr. Matthew Green: Thank you very much.

In your opening remarks I noted that you stated that you wanted to highlight that the RCMP is fully engaged with the Privacy Commissioner's office to ensure that privacy impacts are assessed for all new uses of facial recognition being considered. That's not what we're here for today.

What we're here for today—and perhaps you misspoke in your opening remarks—are on-device interception tools. We heard in the first segment this morning that the Privacy Commissioner was not, in fact, informed on the subject matter of this meeting.

Would you care to comment on the clear and obvious contradiction that you've presented in your opening statement with the testimony as provided by the Privacy Commissioner in regard to what it is we're here for today, which is the on-device interception tools?

● (1535)

Hon. Marco Mendicino: First, I want to thank you for the question, Mr. Green.

I want to acknowledge that it is unfortunate that the Privacy Commissioner has reported that he learned about the use of this particular investigative technique in the media. That is something that I have discussed with the RCMP, and I am pleased to report to you and all members of the committee that they are now actively engaged with the Privacy Commissioner to ensure that the use of this technique—which, again, is used quite sparingly and only after great rigour with the approval of a superior court judge—is done in a manner that is consistent with the charter.

Mr. Matthew Green: As I'm sure you heard in the Privacy Commissioner's opening statements—or your staff would have briefed you on the testimony—that he suggested as a recommendation that the submission of privacy impact assessments to his office be a legal requirement. Would you support and agree with that?

Hon. Marco Mendicino: Mr. Green, I invite and support the work of this committee to offer any recommendations it thinks will augment transparency. I would say to you, as I have said in prior answers, that there are already a number of mechanisms that assure transparency, but I think, given the sensitivity of this technology, given how sparingly it is intended to be used, and again, only with the approval of a superior court judge on the strength of an affidavit that is put forward by a designated agent, we should always be open to having a conversation on how we can raise the bar.

Mr. Matthew Green: Well, we're talking about it now, so I'm going to put the question to you directly. Would you, as the minister responsible, support having it included as a legal requirement, given that we're going to be contemplating a new and revised Privacy Act?

Hon. Marco Mendicino: Mr. Green, I'm happy to say to you that I will be pleased to consider all of the committee's recommendations. I think it's important that we look with great scrutiny and with great merit on the suggestions that you will provide. I also want to make sure, Mr. Green, that as we take your recommendations, we are weaving them into the overall landscape and architecture that is designed to ensure that there is transparency within NSIRA, within—

Mr. Matthew Green: We noted that the Treasury Board has within its policies an open-by-default mandate, one that would have departments proactively engaging with the Privacy Commissioner on issues such as this, and yet, when you look at study of the Health Canada's use of mobile device data that we had to conduct, when you look at Clearview AI, when you look at what's before us here today, what you'll note is a habit of constantly playing catch-up with what these departments are doing.

There doesn't seem to be a culture of transparency and openness by default in this government, and it doesn't seem that these departments are willing to, in a proactive way, engage with the Privacy Commissioner. This is now the third situation that I think could have been avoided at committee, quite frankly, if these agencies had gone on record and pursued privacy impact assessments with full engagement and full co-operation. Would you not agree?

Hon. Marco Mendicino: I think what you'll hear from RCMP officials who are there and what I will transmit to you personally, Mr. Green, is that we always have to be prepared to up our game on transparency. There is the annual report on the use of electronic surveillance, which I think we should look at as one of a series of tools so that we can shine a light on how we use these investigative techniques to protect Canadians. I look forward to the suggestions that you and other members may have, Mr. Green, because I think to build trust and confidence, we need to be transparent.

Mr. Matthew Green: I appreciate that.

I'd like to know specifically what laws and policies are in place to ensure that the tools and new technologies used by the RCMP meet privacy standards under your purview as the minister responsible.

Hon. Marco Mendicino: Well, first and foremost, there are the provisions under the Criminal Code, which, again, contain great rigour and require great transparency and full, frank and fair candour to the court. Second, there's the Privacy Act. Third, I would point out—

Mr. Matthew Green: Do you not agree that those agencies also have a duty of candour to the House of Commons and at committee?

Hon. Marco Mendicino: Without question, Mr. Green. I'm not—

Mr. Matthew Green: Okay, I want to reference for you, now that we have you here before us, the fact that in our previous studies, in fact, we had members of the RCMP refusing to even name what was already publicly available, the person who is responsible for procuring Clearview technology. We have a culture that has been reflected in the courts as being cavalier, which came through in a judicial decision commenting on both CSIS and the RCMP.

What are you doing as the minister responsible to ensure that the duty of candour results in our being presented with full, frank and completely transparent accounting at this committee and the House of Commons?

Hon. Marco Mendicino: In short, I hold all branches within my portfolio accountable for those values you just stated, making sure that the mechanisms are designed and are delivering the transparency that is required to build trust and confidence. It is an ongoing exercise that constantly requires reflection, especially as we—

Mr. Matthew Green: Let me ask you this last question. We talked about the Privacy Act. We talked about having privacy rights embedded in the preamble. We have now determined that the preamble is actually not legally binding. Would you support putting privacy rights within the actual legal framework of the upcoming Privacy Act?

● (1540)

The Chair: Mr. Green has used all of his time without leaving time for an answer. Maybe he can answer—

Mr. Matthew Green: I'll give him time to reflect on that and then reflect back in my next round.

The Chair: Minister, you can give us a quick yes or no to that if you'd like to. I'll let you. Otherwise, we're going to go to Mr. Williams.

Mr. Matthew Green: You can go.

Hon. Marco Mendicino: The short answer, Mr. Chair, is that there are charter and privacy protections already built in, but I invite future recommendations as this committee may submit.

The Chair: With that, I'll go to Mr. Williams.

Mr. Ryan Williams (Bay of Quinte, CPC): Thank you, Mr. Chair.

Minister, thank you for being with us today.

This morning we had Canada's Privacy Commissioner in the room, who spoke about maintaining trust in our public institutions.

Do you believe in maintaining trust in our public institutions?

Hon. Marco Mendicino: Absolutely.

Mr. Ryan Williams: You stated in your opening statements that this technology that you know of has been implemented since 2017. Is that correct?

Hon. Marco Mendicino: That's what I had been advised.

Mr. Ryan Williams: Minister, is it acceptable to you that it's been five years that the RCMP has not submitted a privacy impact assessment and that they are just completing one now? The Privacy Commissioner thought that it would be provided at the end of August. Is it acceptable that it's been five years since they've had that completed?

Hon. Marco Mendicino: As I have said previously, I think it is unfortunate that the Privacy Commissioner was just recently engaged, but I also want to clarify to you and to members of the committee that privacy protections are afforded and complied with in the context of the use of this technology when officers apply for judicial authorizations. That's one of the important—

Mr. Ryan Williams: Minister, my question was: Do you find it acceptable that it's been five years? Again, based on the fact that the commissioner this morning stated that he only learned of this in June—and we think June is probably too long—is five years too long?

Hon. Marco Mendicino: I want to make it abundantly clear to you that when these techniques are used, including ODIT, there has to be a balancing—

Mr. Ryan Williams: Minister, yes or no is absolutely acceptable. Yes or no?

Hon. Marco Mendicino: I've already said that there is privacy protection built into each and every instance when these techniques are used.

Mr. Ryan Williams: Sir, if you're not going to answer my questions, I don't know why we're asking them.

It's very simple. If we have a privacy commissioner asking for very basic instances from our institutions—and you've clearly stated that we want to have trust in our institutions—would it not be acceptable that we ensure, as much as we can in the government, that we have the very basics concluded by those institutions?

Hon. Marco Mendicino: Of course. That's why I've said that—

Mr. Ryan Williams: Thank you, sir, very much.

Hon. Marco Mendicino: —we are engaged with the RCMP—I'm sorry, with the Privacy Commissioner.

Mr. Ryan Williams: Thank you very much, sir.

This committee has been studying, as you mentioned in your opening remarks, facial recognition technology and data mobility. Technology is continually evolving. This is just the latest instance. As you mentioned, 2017 was when this technology came into effect, so we assume there's a lot more of this technology in effect.

To your knowledge, do you know of any other departments under your purview that we should be looking at and for which we should be pushing for privacy impact assessments at this point?

Hon. Marco Mendicino: I would not want to preempt the independence of your committee and whom you wish to study. I would invite, though, the conversation we are having right now on how we can ensure that we are protecting privacy.

There are protections that already exist, but there are mechanisms that I think we can continue to modernize as we use new technology to subvert the efforts of criminal organized actors and other bad actors who would seek to undermine the health and safety of Canadians.

Mr. Ryan Williams: Minister, would it help that Canada's privacy laws be updated quickly? This is something you've been asked, not just on this testimony today but in past testimony. Is that something you think we should be trying to push through a little quicker?

Hon. Marco Mendicino: I think we should always be looking at ways to ensure that Canadians' privacy is being protected. Again, I encourage the study that you are undertaking right now.

Mr. Ryan Williams: Minister, when we talk about the procurement of such technology—obviously someone makes those decisions—is your office aware of those decisions when they're made?

Hon. Marco Mendicino: There are a number of different procurements that are undertaken by independent operational decisions, which, for good reason, lie within the purview of the RCMP. You don't want elected officials conducting investigations.

That having been said, where there are requests for certain types of technology or additional resources, those are usually appropriated under budget requests or other requests. When those are submitted, we obviously evaluate them on the merits.

Mr. Ryan Williams: Thank you, Minister.

Are you aware of CSIS or CSE or any other institution using this technology you've mentioned today?

● (1545)

Hon. Marco Mendicino: I can speak for my portfolio. As I said, the RCMP has said that this is a technique that is used.

Mr. Ryan Williams: Okay.

Are you aware of anyone else using it at ths point?

Hon. Marco Mendicino: Certainly, when techniques like this are used by the government, they are done in a manner that is consistent with the charter, with privacy laws and with all the other mechanisms and transparency attached to it.

Mr. Ryan Williams: Thank you, Mr. Chair.

The Chair: With that, next we go to Mrs. Valdez for five minutes.

Mrs. Rechie Valdez (Mississauga—Streetsville, Lib.): Thank you, Chair.

Thank you, Minister, for joining us today.

Minister, part VI of the Criminal Code sets out the authority for the lawful electronic surveillance mandate of the RCMP. As with any sort of search and seizure, the Criminal Code does not provide the authority for mass surveillance, but grants law enforcement these tools only when absolutely necessary to maintain safety and security.

Minister, can you advise this committee on the threshold needed for the interception of private communications, per the Criminal Code?

Hon. Marco Mendicino: It's a very high one, Ms. Valdez, as you have already mentioned. It is not an easy test to meet. There are only specific individuals, who are authorized under the law, who can bring forward an application for judicial authorization to conduct a wiretap or to utilize some of the investigative techniques that are the subject of this study. It requires that the offence for which there's an expectation that information or evidence might be procured through the technique falls within a very limited number of serious offences under the Criminal Code.

As we already mentioned, Ms. Valdez, the state has to go to some length to demonstrate that this technique, this form of surveillance or search and seizure, is not a first resort and not a tool of convenience but rather is only requested after other efforts have been exhausted. Many protections that are built into the Criminal Code and the law generally are there to achieve the balance between allowing the state to protect individuals while at the same time protecting the individual privacy of all Canadians.

Mrs. Rechie Valdez: You highlighted in your opening remarks the importance of transparency, privacy and accountability. We as Canadians need this from our intelligence agencies. How can we assure Canadians that we respect their right to privacy and their rights set out in the Charter of Rights and Freedoms, and how are those being upheld?

Hon. Marco Mendicino: I think the short answer is that it's by continuing to demand openness and transparency and accountability. That is why I'm pleased to appear before you and the other members of this committee. I invite the study that you are undertaking right now. I think it is important that we explain to Canadians why law enforcement has to resort to this technology. In turn, it's because criminals and bad actors are getting better at finding ways to avoid detection by law enforcement, whether it's through encryption or through other sophisticated techniques. They don't want to be caught. They want to get away with it.

We know that the consequences can be devastating, particularly as we start to live out more of our lives online. These are not technologies that are being deployed as a matter of convenience, or lightly or frivolously. These are technologies that are being deployed by the state to protect the security, safety and health of Canadians. As we deploy those techniques and those technologies, I think it's important that we shine a light, as much as we possibly can, without compromising operational integrity. There is a balance to be struck there, but to circle back to the original premise of your question, we can build confidence among Canadians if we are open with them.

Mrs. Rechie Valdez: Thank you.

In March 2021 our government created the national technologies onboarding program to bring more transparency to the RCMP and how they gather, identify and track new and emerging technologies. Can you give the committee some oversight on how this program works and how the RCMP maintains that right to privacy while conducting their investigations?

Hon. Marco Mendicino: In plain terms, it's meant to centralize these processes. By centralizing them, we can ensure that there's greater compliance with professional standards, with the law. Chief members of the RCMP have been designated to apply for the use of these techniques. They're very much up to speed on what is required by the court...making sure that they're kept abreast of any developments in the law, because on occasion the courts will clarify on how the law should be interpreted, depending on the techniques being used and the technology being used, and how they are interpreting on how we strike that balance appropriately.

Centralizing through the NTOP does allow for, I think, a higher level of confidence that the members of the RCMP are adhering to the rigours of the law with highly trained individuals who are adhering to high professional standards.

● (1550)

Mrs. Rechie Valdez: Thank you.

Chair, I think that might be my time.

The Chair: You have time for another question, if you like. You have about 35 seconds left.

Mrs. Rechie Valdez: Let me try to squeeze this in.

Minister, at the end of the day, Canadians want to know that their privacy, their families and their rights are protected. How can we continue to assure that this is going to happen for Canadians?

Hon. Marco Mendicino: It will be by making sure that we have laws that protect their privacy; by making sure that we adhere to the mechanisms of transparency; by co-operating with NSIRA, NSICOP and the Privacy Commissioner; and by continuing to engage with all parliamentarians, including this committee, so that we can have an open and frank discussion about how we protect Canadians with new technologies while respecting their rights under the charter.

Mrs. Rechie Valdez: Thank you.

The Chair: All right. That will do it.

Now we will go to Monsieur Villemure.

[*Translation*]

You have two and a half minutes.

Mr. René Villemure: Thank you, Mr. Chair.

Mr. Minister, is it possible to provide the committee with all the reports you mentioned a little earlier? That would be very helpful, because it would save us a lot of hours of research.

Hon. Marco Mendicino: That's entirely possible.

Mr. René Villemure: Thank you very much.

You talked about openness, transparency and accountability. We agree that these are good things. All of these things are done to gain the public's trust. We agree with that.

The government has made a commitment to transparency and national security, while emphasizing that it will be transparent, but that it will not always be able to provide details. We understand that.

Based on what you said earlier in your opening remarks, efforts are being made to ensure transparency.

Pardon me for saying this, but we have to take your word for it. I'm wondering if having to take your word creates trust.

What do you think?

Hon. Marco Mendicino: I agree that if we want to maintain people's trust, we need to be open and transparent. That is why the work of this committee is essential.

It is also essential that the RCMP and the commissioner work together to protect privacy rights. That's why we must continue to work with the National Security and Intelligence Review Agency and the National Security and Intelligence Committee of Parliamentarians. It's only through transparency—

Mr. René Villemure: I'm sorry for interrupting you, but my time is limited.

My colleagues mentioned facial recognition and data geolocation. It seems to me that the culture of the RCMP is one of avoidance rather than privacy.

What do you think?

Hon. Marco Mendicino: I hope and believe that the RCMP understands and abides by the commitment to be transparent and to always work collaboratively with all the institutions that are there to protect the charter rights of Canadians.

The RCMP will continue to work in good faith with all parliamentarians, and it will continue to work hard. It will continue to work with this committee to ensure that the value of transparency is respected and to help build trust.

Mr. René Villemure: Would you be prepared to ban Pegasus in Canada?

Hon. Marco Mendicino: Yes.

Mr. René Villemure: Thank you very much.

[*English*]

The Chair: We'll go to Mr. Green for two and a half minutes.

Mr. Matthew Green: Thank you very much.

From some disclosures that we had in preparation for this committee, we noted that there were 32 instances of this technology deployed dating back to the year 2017. In your briefing notes, was it ever disclosed to you that there were instances that were before the date of 2017?

Hon. Marco Mendicino: Mr. Green, I've been advised that the earliest year in which this technique was used was 2017.

Mr. Matthew Green: In the testimony of the Privacy Commissioner, when we were referencing the use of stingray technology, which sets up phantom cell towers to intercept cellphone information, it was noted that there were instances where the use had happened without a warrant.

Are you aware of any instances when this might have been used? I think it was exigent circumstances or something to that effect. Are you aware of any instances where that would have happened?

Hon. Marco Mendicino: I think the precise test would be whether or not there were exigent or emergency circumstances, but it is my knowledge that these have all been subject to prior judicial authorization. I would invite you to put the question directly to the RCMP as well.

● (1555)

Mr. Matthew Green: When I asked this question, respectfully, I felt like you kind of danced around it. Again, one of the ways in which I think this committee would avoid much of the work we've already done is if we had a system in place that allowed for privacy impact assessments to happen as a legal requirement through the Privacy Commissioner. I'm going to ask you once again: Is that something you would support, given the work of this committee and the testimony that you've already given on the importance of privacy as a fundamental right?

Hon. Marco Mendicino: Mr. Green, I guess what I'm getting at in my answer is that I look forward to receiving that recommendation. I think—

Mr. Matthew Green: That's the same answer.

I'm going to ask this next question in a direct way. When the privacy impact assessment is provided to the Privacy Commissioner, would you be willing to turn that over to this committee, given the foundation of the duty of candour and the power of this committee to send for documents and evidence?

Hon. Marco Mendicino: Yes. I mean, I think I want to be as transparent as I can be about those privacy impacts. I also want to make sure that we're respecting the process that is being undertaken by the Privacy Commissioner in conjunction with the RCMP. The bottom line for me is that I think the more transparent we can be, the better.

The Chair: Thank you.

With that, we will go to Mr. Kurek for five minutes, followed by Mr. Bains for five minutes. That should conclude this panel.

Go ahead, Mr. Kurek.

Mr. Damien Kurek (Battle River—Crowfoot, CPC): Thank you very much.

Thank you, Minister, for coming here today.

You avoided answering the question before, so I'll maybe direct it to you in a little bit of a different way. Are you aware of any other instances of agencies or departments under your purview that have utilized this technology—yes or no?

Hon. Marco Mendicino: Again, I would say to you that—

Mr. Damien Kurek: Other than the RCMP, Minister, are you aware of any entities under your purview—I'm not even asking you to identify those departments—that have used this technology? That's other than the RCMP.

Hon. Marco Mendicino: I was coming to the answer. I was just in the process of saying that these techniques, if and when they are used, are always done in a manner that is consistent with the law and the charter.

Mr. Damien Kurek: We'll take that as a "yes", although with some equivocating on how you came about it.

Minister, as has been the case, and certainly as I've seen a number of times before this committee, the government's response seems to be that we need to build trust, so just trust us. In many cases, including the contradictory testimony you've given here today with what the Privacy Commissioner spoke about this morning...and seeing how the OPQ signed off on by, I believe, your parliamentary secretary at the time, Ms. Damoff, and the letter that was provided to this committee, there's a difference. There's a discrepancy that exists.

There are provisions within both the Criminal Code and other legislative frameworks that allow for national security to be used to circumvent part VI and the normal judicial processes required for surveillance operations. Minister, yes or no: Are you aware of that ever having been used while you've been Minister of Public Safety—yes or no?

Hon. Marco Mendicino: I just want to be very clear that when these techniques are used, they're done in a manner that is compliant with the law. I've set out on a number of occasions how—

Mr. Damien Kurek: Minister, I think my question was quite direct. There are national security exemptions that can be used to circumvent the typical processes. There's that judicial process, which you've expounded on quite fulsomely, within part VI of the Criminal Code. There are national security exemptions where these surveillance techniques can be used without fulfilling the full process outlined in part VI of the Criminal Code. To your knowledge, are you aware of that ever having taken place while you've been Minister of Public Safety—yes or no?

Hon. Marco Mendicino: I would just again point out that when this technique is used, it's done in a manner that is compliant with the law and the charter. For any additional details, I would invite you to put those questions directly to the officials who are there to provide those answers.

Mr. Damien Kurek: With respect, Minister, you are the elected official, the cabinet minister, who provides that oversight that Canadians expect. The fact that there have been less than direct answers I think is very, very telling of that culture of secrecy that seems to be involving.... Certainly, I hear often from constituents who are frustrated with the actions of this government when it comes to its unwillingness to be forthcoming with what I think are very, very simple questions.

Minister, we see specifically some of what the Privacy Commissioner spoke of this morning, that it's only been after the media reported on this ODIT technologies being used that the RCMP...that now the Privacy Commissioner is engaged with the RCMP. Does it concern you that this confirms a trend, which we've seen from your government, where only after public scrutiny, and in many cases parliamentary and media criticism, is action taken to, in your words, "build trust and confidence" of Canadians?

● (1600)

Hon. Marco Mendicino: As I have previously expressed, I think it's unfortunate that the Privacy Commissioner found out through the media. That's why I'm inviting the work that is being done today. As I've said before, we should always look at ways in which we can raise the bar on transparency, particularly as we're using new technologies to protect Canadians.

Mr. Damien Kurek: There's a lot that's unfortunate. Certainly, I do look forward to tomorrow morning with the previous Privacy Commissioner, who has had—I would note for the record, Mr. Chair—very, very public disagreements with the RCMP among other instances.

Minister, I hope you can appreciate that Canadians are not comfortable with the simple comments that this government seems to say—we're building trust, so just trust us—and I hope we can certainly get to some answers in this regard.

Hon. Marco Mendicino: Well, I would just say to you that there are many mechanisms of transparency to ensure that there is openness, including NSIRA and NSICOP and the very rigorous tests under the Criminal Code. That's how we'll continue to build transparency in addition to the good work of this committee.

The Chair: Thank you.

The final member in this round will be Mr. Bains.

You have five minutes. Go ahead.

Mr. Parm Bains (Steveston—Richmond East, Lib.): Thank you, Mr. Chair.

Thank you, Minister, for joining us today. Thank you for being very forthcoming and telling us about the various transparencies that are available.

In my first question, I would like to ask you about facial recognition. We've heard from experts that facial recognition technologies inherently further racial biases, misidentifying racialized individuals at a much higher rate. If the RCMP is making use of such technologies, how are they accounting for these discrepancies and addressing these systemic inequalities?

Hon. Marco Mendicino: Thank you very much, Mr. Bains, for the question. As part of my mandate, I'm working very closely with the RCMP, and indeed all branches within Public Safety, to address systemic racism and other institutional barriers that for far too long have led to disproportionate outcomes particularly involving racialized Canadians and indigenous peoples.

I would invite the members of this committee to take a look at the most recent and updated mandate letters that I have issued to all branches within my portfolio, including the RCMP who are here before you, because we have to tackle this work together. I want to commend the commissioner and all of the members of the executive team for understanding and appreciating that it is a top priority for our government to do just that. We obviously have a long way to go. I don't want to give this short shrift. I know that the committee is looking at a very specific issue, but I completely take your point that the institutional barriers to systemic racism have been a real problem and have plagued all of our institutions, including law enforcement, for far too long. We're looking to right the ship.

Mr. Parm Bains: Thank you for that.

You mentioned the national technologies onboarding program. Can you provide this committee with an understanding of how this program will provide greater oversight on the use of technologies and investigative tools used by the RCMP?

Hon. Marco Mendicino: Thank you for the question, Mr. Bains. I think in some ways I discussed this previously with the question from Ms. Valdez.

In essence, what the RCMP have done is they have created this branch or this particular office, if you will, to centralize our efforts in the use of this technology. By doing so, we can be sure that there are very clear and high expectations set with regard to professional standards; that there is training provided to those members who have been designated to apply for the use of this technology; and that, as part of that training, they are kept abreast of any developments in jurisprudence in the law so that where there needs to be improvement, where there needs to be course correction, and where there needs to be greater sensitivity to ensure that we're protecting privacy, we are adhering to those values.

As I think we've heard throughout today's conversation, one of the running themes is that we all want to build trust and confidence, but in order to do that, there needs to be transparency, openness and accountability. I think the creation of this office is designed to do just that.

● (1605)

Mr. Parm Bains: As a follow-up to that, what involvement, if any, do you have with the RCMP decision-making process as it relates to the decision to use ODITs in a particular case?

Hon. Marco Mendicino: None—these are operational techniques. We don't want elected members of the government, or any elected politician, for that matter, directing or trying to steer investigations, which by extension would include investigative techniques or judicial authorizations. There are safeguards, including constitutional principles, which have been established by the Supreme Court to safeguard operational independence. That is something that I believe, and I hope it's something that all of the members of this committee believe. You don't want me or any other elected member directing the use of this technique.

Mr. Parm Bains: Thank you.

Do I have any more time, Mr. Chair?

The Chair: You have almost a minute. If you'd like to ask another question, go ahead.

Mr. Parm Bains: Okay.

Minister, in your view, what advances in encryption technology convinced the RCMP that traditional means to monitor the communications of possible criminals were no longer sufficient?

Hon. Marco Mendicino: The emergence of countersurveillance technology, like encryption, is being used by criminal actors and bad actors who are trying to undermine public safety and national security. It is through the detection of those countersurveillance techniques and technologies that law enforcement and RCMP have had to help and utilize other techniques to make sure that we can bring to justice those who are trying to do harm to Canadians.

It's very difficult. It's complex work. But there are protections that are built into place, including tests under the law and other transparency mechanisms, so that we can accomplish that balance.

The Chair: All right. Just before I suspend the meeting to transition to the next panel, I would like to thank the minister for his time and his willingness to appear at committee.

With that, the meeting is suspended.

● (1605)

_____(Pause)_____

● (1610)

The Chair: Welcome back. I'm going to convene the second panel of today's meeting.

With us for the second panel, from the RCMP, we have Mark Flynn, assistant commissioner of federal policing, national security and protective policing; Bryan Larkin, deputy commissioner of specialized policing services; and Sergeant Dave Cobey, technical case management program, technical investigation services.

We will begin our second panel with opening statements from the RCMP.

Go ahead, for up to five minutes.

[*Translation*]

Deputy Commissioner Bryan Larkin (Deputy Commissioner, Specialized Policing Services, Royal Canadian Mounted Police): Thank you.

[*English*]

Good afternoon, Mr. Chair and honourable members of the committee. The RCMP is grateful for the opportunity to speak with you today about this important matter. We hope that our comments will inform your study into the RCMP's use of on-device investigative tools, commonly known as ODITs.

Encryption is essential in our modern world. It protects financial and other sensitive information and helps ensure that Canadians' online activities remain safe and private. Unfortunately, encryption and the devices that help protect Canadians' privacy also help criminals conduct illegal activities and avoid police detection. Although police are sometimes able to collect data stored on those devices, encryption often renders the data unintelligible.

Before I go into detail on what ODITs are, I would like to be clear that the RCMP has never procured or used the Pegasus software, or any other NSO product.

ODITs are used extremely rarely and in limited cases. Their use is always targeted. It's always time-limited, and it's never to conduct unwarranted and/or mass surveillance. These tools are not used in secret. ODITs require judicial authorization prior to deployment, and the evidence collected, including how it was collected, is subject to disclosure and court scrutiny.

Given the RCMP's mandate, we are not able in this setting to discuss specific operational requirements, and the RCMP is not able to disclose sensitive details related to the tools and techniques used in the course of its investigations. Any public disclosure beyond the technical documentation that we provided to the committee that describes the general capabilities of an ODIT has the potential to adversely impact our investigations.

Our use of ODITs is in full compliance with Canadian legislation, including the Charter of Rights and Freedoms, the Criminal Code of Canada and established jurisprudence.

ODIT technology may be used to assist in high-priority investigations relating to national security, serious and organized crime, and other Criminal Code offences that impact the safety and security of all Canadians. It will only be deployed after judicial authorization has been obtained.

As for what an ODIT is, an ODIT is a computer program that's installed covertly on the cellphone and/or computer of a suspect.

ODITs assist investigations by maintaining law enforcement's ability to covertly collect private communications and other data that can no longer be acquired using traditional wiretaps and/or less intrusive investigative techniques. The amount and type of data collected is determined on a case-by-case basis in accordance with strict terms and conditions imposed by the judge who authorized the use of the ODIT.

The RCMP's cautious and measured approach is evidenced by the fact that since 2017, ODITs have only been used in support of 32 investigations, in which a combined total of 49 devices were targeted. Again, I emphasize that in the past five and a half years, we've targeted 49 devices for ODIT deployment.

The RCMP carefully considers the advantages and disadvantages, including the impact on privacy and third parties, before seeking judicial authority to use ODITs in support of a criminal investigation. That assessment is conducted in close collaboration with investigators, technical specialists and federal and provincial Crown prosecutors. It is overseen by our technical case management program within RCMP headquarters. Again, we stress that ODITs are only used for serious criminal offences, and only as approved by a judge who explicitly authorizes the use of ODIT on a specific suspect's device. Judges receive and continue to receive supporting material explaining what the ODIT is and its capabilities.

Although we are not able today to disclose the name of organizations with whom we work in a public setting, we would like to again confirm that the RCMP has never procured or used Pegasus or any other NSO product. Sharing details publicly exposes sensitive information that could negatively impact the RCMP and our public safety partners' ability to effectively use ODITs in the future. Criminal elements also use this sensitive information in order to render the tools ineffective. Further, in addition to negatively impacting the RCMP's investigations, the exposure may jeopardize the investigations of foreign partners and our relations with those countries.

In April of this year, we provided a detailed briefing on the RCMP's use of ODITs to Canada's National Security and Intelligence Review Agency. On August 23, representatives of the Office of the Privacy Commissioner of Canada will also receive a similar briefing.

I would like to bring to the committee's attention that on July 4, 2022, the National Security and Intelligence Committee of Parliamentarians—NSICOP—notified the Minister of Public Safety of its decision to conduct a review of the lawful interception of communications by security and intelligence organizations, which we will fully participate in. The objectives of the review include examining the current state of lawful access, concerns raised by civil society and privacy experts, technological challenges, as well as the gaps. On the basis of its review findings, NSICOP may make recommendations pertaining to various aspects of lawful intercept activities and frameworks.

● (1615)

The Chair: I'm so sorry, Mr. Larkin, but I've let you go significantly over the time allotted for opening statements. Your testimony is important, but we're going to have to get to questions from members.

Even before we do that, I will say on behalf of the committee that voted for some very specific information from the RCMP that it was quite disappointing, in fact, troubling, to receive in Commissioner Lucki's letter what amounts to just a point-blank refusal of information.

As Canada's grand inquisitor, a committee of Parliament has unfettered power to request documents. We can have a discussion about the appropriateness, and you touched on that in your remarks. I look forward to the discussions that we'll have from the parties about that, but a blanket refusal to a committee is troubling. We'll get to that, I'm sure, with questions from committee.

With that, I will go to the first round that will begin with Mr. Bezan.

Mr. James Bezan: Thank you, Mr. Chair.

I want to thank our witnesses for being here.

I thank the RCMP for their work.

We on the Conservative side here do believe that we want to make sure you guys have the tools to do the job so that you can keep Canadians safe and deal with issues of national security and public safety at all times, but there's also the need to protect the rights of Canadians, the privacy of Canadians and their charter rights. There are concerns about the unintended consequences of deploying ODITs and the potential that those who aren't necessarily being targeted are also being spied on using the technology that you have.

There has also been confusion here, because when we had the response to the Order Paper question tabled by the RCMP via the parliamentary secretary to the Minister of Public Safety in the House back in June, it talked about 10 or 12 cases where ODIT was used. Then, in the rather disappointing letter that came from Commissioner Lucki, it talks about 32 investigations. Now you're saying that there were 49 individuals who were spied on. The number continues to move, Mr. Larkin, and we're all very concerned about where the truth lies. I think that's why we need to have better clarity on the information we have.

We already know that you're not using Pegasus, but you do have a technology. Is it made in Canada? What's the country of origin of this technology that you're using in your investigations?

● (1620)

D/Commr Bryan Larkin: Thank you so much, Mr. Bezan.

I would just like to clarify that we have deployed 32 applications targeting 49 devices, not 49 individuals. That's just a point of clarification.

I will defer to Assistant Commissioner Mark Flynn to discuss the technology and the procurement of such.

Assistant Commissioner Mark Flynn (Federal Policing, National Security and Protective Policing, Royal Canadian Mounted Police): Within the RCMP's technical investigative services, there is a process under which they procure all technology. There's an approval process where there's director general level approval for both the procurement of the tools and techniques, as well as approval of which particular tools and techniques can be utilized by the RCMP and our covert electronic surveillance.

Mr. James Bezan: You cannot disclose whether it's Canadian technology or the country of origin of the technology? If it's not Pegasus, then where does it come from?

A/Commr Mark Flynn: From my perspective in federal policing, I'm not aware of where all the technology comes from that's utilized here, but I can say that I have a long-standing history in this, and back in the days from 2002 to 2015, it was all Canadian technology that we were utilizing, but—

Mr. James Bezan: This predates what we're talking here. It was 2017 for ODITs, so are you saying that we've been using this technology since 2012?

A/Commr Mark Flynn: I can add some clarification to that. It goes back prior to 2012. I can add some clarification to that when you're ready.

Mr. James Bezan: So we use this technology, hopefully respecting part VI of the Criminal Code that charter rights have been protected.

How often have you used it under national security provisions where you don't have to get a warrant, going back to 2012 or before? We're talking ODIT and we're also talking, I believe it was your special investigation unit “I”, right?

A/Commr Mark Flynn: From my involvement, again going back for many years as well as my current position in national security, we have never utilized this tool without prior judicial authorization.

Having said that, if a situation were to arise that required it, there are provisions that allow us and certain designated individuals to utilize this type of tool for the interception of communications in emergency situations, but I am not aware of any situation where that has been done, and the mere practicality of deploying this type of tool and technique would take it beyond the time period under which such an authorization would be valid.

Mr. James Bezan: When it is a national security issue, or it's somebody like Canadian Navy former lieutenant Jeffrey Delisle back in 2012, are you saying that this would have been probably used in that situation? Knowing that he was a member of the Canadian Armed Forces, knowing that there may be people of interest within the RCMP, do you still have to go through the process of getting a warrant to protect their charter rights and the Criminal Code part VI, or can you on staff surveil them or use spyware without their knowledge and without the consent of the justice system?

A/Commr Mark Flynn: I can say unequivocally that in that case and in any other similar case, we have utilized the prior judicial authorization for doing so, and not obtaining such judicial authorization would be a violation of Part VI of the Criminal Code because part VI contains the privacy invasion provisions under the code and we would not do that. We are a professional organization that operates under the law.

Mr. James Bezan: As a professional organization that has used a type of spyware since 2012 or sooner, why did it take until it became public information? Why did you never consult with the Office of the Privacy Commissioner before that?

A/Commr Mark Flynn: I can speak again from a long-standing history in the Special “I” program, and as we follow through the evolution of the use of this technology, as encryption started to be used by targets that we had judicial authorization to intercept, and we were unable to hear the audio, hear the phone calls or see the messages they were sending, that is when we developed the tool and technique to make it possible to intercept those communications.

But it's important to note the privacy invasion isn't coming from the tool utilized. The privacy invasion is coming from capturing that audio or capturing that text message or capturing that communication that is occurring between two individuals, and we have evolved in the use of the tools as individuals evolve in the way they communicate.

● (1625)

Mr. James Bezan: So—

The Chair: Thank you. No, you're over time a fair bit there, but I wanted to let that answer go—

Mr. James Bezan: Thank you.

The Chair: —without interrupting, but we must now go to Ms. Khalid for up to six minutes.

Ms. Iqra Khalid: Thank you, Chair, and through you, thank you to our witnesses for appearing today.

Just to put all of this into context, I'll start by asking how many investigations have been conducted by the RCMP in general over the past five years?

Sergeant Dave Cobey (Sergeant, Technical Case Management Program, Technical Investigation Services, Royal Canadian Mounted Police): Chair, through you, are you asking about the total number of investigations?

Ms. Iqra Khalid: Yes, the total number of investigations.

Sgt Dave Cobey: As I sit here right now, I don't know that number, but it would be a very large number.

Ms. Iqra Khalid: Okay, and out of that very large number, how many of those investigations used ODITs? I heard it was 32 or 35, and I just wanted to clarify that.

Sgt Dave Cobey: Yes, since 2017, only 32 investigations have used ODITs.

Ms. Iqra Khalid: And how many of those investigations were conducted without a warrant?

Sgt Dave Cobey: Mr. Chair, through you, every one of those 32 investigations had a judicial authorization to use ODITs.

Ms. Iqra Khalid: And what kind of criminal activities were in question the times that ODITs were used within these specific cases?

Sgt Dave Cobey: Mr. Chair, I believe that information was in the package that was provided.

It breaks down into several different types. The most investigations are related to terrorism or serious drug trafficking investigations. There were also five murder investigations and there were also some breach of trust investigations, one of those being the investigation of a police officer's activities. But for the total, all combined, there were 32, and all 32 investigations had at least one offence that was under section 183, which the minister mentioned the previous meeting. Those are all serious offences.

Ms. Iqra Khalid: Thank you.

The RCMP is subject to the Privacy Act. What practices do you use in general within your department to ensure that your device investigation tools comply with the Privacy Act?

Sgt Dave Cobey: I can say, as of most recently when we initiated our national technology onboarding program, really, the genesis of that program was the OPC's report of Clearview AI. As a result of that report, one of the recommendations that the OPC made and which the RCMP agreed to implement was to have a more centralized process to ensure all privacy-related considerations were followed, including assessing early in the process whether a PIA is required, and if yes, ensuring that PIA is written as well as other internal RCMP requirements related to data security, and whether a warrant is required. If a warrant is required the terms and conditions and language needed to properly describe technologies are included in that warrant and things like that.

Ms. Iqra Khalid: We heard from the OPC earlier today that it took a while for the RCMP to get to them. Why is that?

Sgt Dave Cobey: I'm not sure, in specific terms, about the ODIT in particular, but I can tell you that following the OPC investigation and since NTOP has been established, we're working to redouble our efforts to identify these technologies as early as possible and, if personal information is implicated, begin the process of engaging the OPC as soon as possible.

Ms. Iqra Khalid: Thank you.

In terms of the scope of ODITs within the investigations, is there a big capacity for people who are not the subject or target of an investigation to be captured within ODITs, for example? Are there any mitigation factors that the RCMP uses to make sure that they're very limited in scope?

Sgt Dave Cobey: One of the attachments you would have received was the sample judicial authorization that we shared with NSIRA for the purpose of their demo. The short answer to your question is that the authorization that gets prepared in relation to an ODIT deployment includes several terms and conditions imposed by the judge, which require us to.... If information unrelated to the investigation or not pertinent to the offences being investigated is captured, then yes, that has to be set aside and dealt with in a protected manner, as well as other information, such as, for example, information related to solicitor-client privilege and things like that.

Many of the terms and conditions included in a regular part VI or wiretap warrant are included and read into our ODIT warrants. As we've used these new tools over the years, we've tried to really take a cautious approach to implementing them to make sure those terms and conditions are followed.

● (1630)

Ms. Iqra Khalid: I'll also ask a question that came up earlier with the minister. It's with respect to racial discrimination. As we've learned through the facial recognition technology, race is a huge component in how surveillance happens. The RCMP is working on this, but it does not have a good track record.

I'm wondering if you have anything to say to that and what measures you're taking as you use technologies like this, within their limited scope, to ensure that there's no racial profiling.

Sgt Dave Cobey: I can tell you, in relation to ODITs in particular, that our technical investigative services unit is a technical support unit that provides assistance to investigations. Our involvement is at the level of assessing the technologies that are implicated in the investigations, as opposed to particular targets. Really, that's not something our unit is in a position to have an impact on, because we're looking at the devices and technical challenges in the collection or interception the investigators are trying to achieve.

The Chair: All right.

[*Translation*]

Go ahead, Mr. Villemure. You now have the floor.

Mr. René Villemure: Thank you very much, Mr. Chair.

I'd also like to thank the witnesses for appearing before us today.

Without compromising national security, but so that the people in the riding of Trois-Rivières can clearly understand some elements, I have a series of questions for you.

My questions are very simple and can be answered with yes or no.

Is the RCMP able to install spyware on a cellphone without the user's knowledge?

[*English*]

Sgt Dave Cobey: Yes.

[*Translation*]

Mr. René Villemure: Is the RCMP able to capture or listen in on a cellphone conversation?

[*English*]

Sgt Dave Cobey: With judicial authorization, yes.

[*Translation*]

Mr. René Villemure: I agree, obviously.

Is the RCMP able to capture or view what can be seen through the cellphone camera?

[*English*]

Sgt Dave Cobey: Depending on the device and our capabilities at the time, the answer can be yes.

[*Translation*]

Mr. René Villemure: Is the RCMP able to consult the information, calendar, photos or text messages, in other words, what's on the cellphone?

[*English*]

Sgt Dave Cobey: With the same caveat, yes.

[*Translation*]

Mr. René Villemure: Great.

Thank you very much.

We heard testimony from the Privacy Commissioner this morning. Earlier, the minister said that you were fully committed to the commissioner.

Before using this software for the first time, did you consult with the Privacy Commissioner, yes or no?

[*English*]

A/Commr Mark Flynn: No.

[*Translation*]

Mr. René Villemure: Okay.

Thank you very much.

I'll continue on another subject.

I was also disappointed with the letter we received the other day from Commissioner Lucki. We had asked a fairly clear question, and we got a very clear response. We had asked if parliamentarians had been wiretapped, and we were told that this information would not be provided by the RCMP.

Do you have anything to add to that?

[*English*]

A/Commr Mark Flynn: I would just add that when we're speaking about any individual in particular, to be asking a question about parliamentarians specifically is a challenging question because it's actually putting the authority of the individuals asking in a position to speak to something that they care about.

We take the privacy of all Canadians, regardless of the positions they hold, to be very important, which is why we put all the protections in place. However, I would add that there are certain sectors—which include parliamentarians, journalists, religious institutions, educational institutions—where we have additional safeguards within our policies and procedures to ensure that a higher level of authority is required if a request is being made or an operational requirement is in place due to the criminal behaviour of the individuals involved that fall within those sectors. It requires a higher level of approval. For national security matters, that is my position as the assistant commissioner in charge of national security.

[*Translation*]

Mr. René Villemure: Thank you very much.

Have any political parties ever been under surveillance?

● (1635)

[*English*]

A/Commr Mark Flynn: Again, that goes back to speaking about particular targets of investigations. I can say that parties themselves.... I have great confidence, without having reviewed—I put a strong caveat on this here—all judicial authorizations, that the RCMP does not target political parties.

[*Translation*]

Mr. René Villemure: Thank you very much. I'm very happy to hear that.

Considering the fact that technologies are evolving rapidly, do you think there should be some kind of moratorium on their use so that people understand what's at stake?

We have to admit that it's complex. Do you think a moratorium is a good idea to allow more people to express themselves and understand what is going on?

[*English*]

A/Commr Mark Flynn: I do not believe a moratorium is necessary.

Again, going back to the point I raised earlier that led to the evolution of the use of this technology, we are talking about the most invasive techniques that we can have when we are speaking about interception of communication, whether that be an analog telephone conversation or an encrypted conversation. The privacy, not the difficulty or the level of complexity in the technology utilized, is what needs to be protected. The RCMP has protected that technology. The laws of Canada have protected that right to privacy, and it does not speak to the level of sophistication required. I think those protections are valid today, as they were back in the 1960s.

[*Translation*]

Mr. René Villemure: Thank you very much.

Mr. Larkin, you mentioned foreign partners earlier. You said that you didn't want to jeopardize outside investigations.

Can you tell us if Canadians may be subject to surveillance by foreign entities?

[*English*]

D/Commr Bryan Larkin: Thank you very much, Mr. Villemure.

I'm going to turn it over to Assistant Commissioner Mark Flynn, who looks after our national security and protective services.

However, with regard to your previous point, I'd like to re-emphasize that the RCMP recognizes that there are gaps in current legislation. We think that the work of this committee is very important to enhancing and mitigating those risks, mitigating those gaps, and we're very open to working in that process about transparency. I think it's very important for us to recognize that as evolution of technology is outpacing our ability to keep up, necessarily there is a required need for enhanced legislation mitigating those risks to allow us to ensure accessibility and accountability, but also ensuring the privacy of Canadians.

I'll turn over your specific question, Mr. Villemure, to Mark Flynn.

[*Translation*]

Mr. René Villemure: Thank you.

[*English*]

A/Commr Mark Flynn: If possible, could you just repeat the key point of the question? I just want to make sure—

[*Translation*]

Mr. René Villemure: Earlier, I heard Mr. Larkin mention foreign partners. I'm wondering if there are any foreign partners—it could be countries—that are currently surveilling Canadians.

[*English*]

A/Commr Mark Flynn: The key distinction I needed to get there was “foreign partners”.

As you'll know, there are agreements internationally with certain partners that there will not be surveillance—amongst, particularly, the Five Eyes—on our citizens.

However, I would say from my position in national security that you must be concerned, that you should be aware that foreign states that are not partners would absolutely be utilizing these types of tools and techniques. I see around this room many electronic devices. All of you are using them as much as anyone in society today, and you must be concerned and must be aware that you are being targeted. I have very little doubt about that.

[*Translation*]

Mr. René Villemure: Thank you very much.

[*English*]

That's a clear answer.

The Chair: Thank you for that candid answer. We went over time on that round, but that was important information.

Now we go to Mr. Green.

Mr. Matthew Green: Thank you.

Who is the ranking officer amongst the three of you?

D/Commr Bryan Larkin: Mr. Green, that would be me as the deputy commissioner of specialized policing. I recently transitioned from a municipal police force as a chief of police—

Mr. Matthew Green: I'm well aware that in the Waterloo region, you've done a lot of work there.

D/Commr Bryan Larkin: —to the deputy commissioner of specialized policing. One of my mandates has been to ensure the work is—

Mr. Matthew Green: I just need the confirmation on that . I do appreciate it. You'll also appreciate that in our timed rounds we have to be expeditious.

You've probably heard me, then, request from the minister responsible that the RCMP provide this committee with the privacy impact assessment that is being prepared right now for the Privacy Commissioner. Being the ranking officer, would you commit to doing that, to hand that over to this committee at the appropriate time when it's prepared?

D/Commr Bryan Larkin: Again, Mr. Green, we're very much open to advancing transparency within the RCMP. We look forward to our meeting on August 23. It's something that we would certainly consider sharing with this committee as we move forward to build transparency and to enhance trust amongst Canadians, so yes.

● (1640)

Mr. Matthew Green: Just so that we're clear, we do have the ability to send for documents unfettered. I'd rather not have to move a motion that would request that document. If I could just get your commitment here on the record today, in the committee evidence, that we can do that.... If there are things within the privacy impact assessment that...I'll have you note that this committee has the ability to go in camera, like NSICOP, like others.

That said, I did hear some referencing, Mr. Chair, to some discomfort with having discussions about the partners and the places of origin for this.

Given that we have your commitment, Mr. Larkin, that you will provide the privacy impact assessment to this committee at the appropriate time when it's prepared, would you be willing to go in camera with this committee to perhaps expand on the use of this technology so that we have access to the same information the government has?

D/Commr Bryan Larkin: Mr. Chair, just to clarify one caveat, Mr. Green, it would be yes on the privacy impact assessment, but also recognizing that there may be sensitive information that would be best shared in camera.

Mr. Matthew Green: Right.

D/Commr Bryan Larkin: Again, we welcome any opportunity, as we're doing with the Office of the Privacy Commissioner and NSICOP, to go in camera to share further details. We're certainly willing to do that. We welcome that opportunity.

Mr. Matthew Green: Okay.

As I'm sure you're well aware, one of Peel's principles is that the ability of the police to perform their duties is dependent on the public's approval of police actions. I think you've been present at the previous interventions indicating that we're having some trust issues.

We had members of your service refuse to provide basic information to this committee, which in my opinion is in contradiction to your duty of candour. I'm hoping that, at the appropriate time, we would get a chance, perhaps, to invite you back in camera to expand on our learning as a committee. Again, we have four meetings. I think there's probably going to be an opportunity to revisit some of this stuff once the privacy impact assessment is completed.

We've heard time and time again, Mr. Chair, from the minister responsible that he is keenly looking forward to our recommendations and, despite some of the protestations of the government members of this committee, is actually excited that we're having this discussion.

If there's a question that I have looming from today, it is about processes of oversight. I reference it in a sample letter. Have you been privy to the sample letter that was provided by the RCMP? It was on a warrant. I referenced it in the morning. It talked about interceptions of on-device investigative tools. It's on page 6:

> d. When oral communications have been intercepted using an ODIT, the monitor who subsequently reviews the communication must cease reviewing the communication as soon as the monitor determines that no person in paragraph 3a is a party to the communication

Would you be willing to go on the record right now and say that this is a standard practice within these warrants, that parameter?

Sgt Dave Cobey: Yes.

Mr. Matthew Green: Okay, I'm seeing the nod. It's on the record, yes.

Who would be responsible for providing oversight that it actually happens?

Sgt Dave Cobey: I see that you have a sample. The warrants are issued by a judge. The technical investigative services would have a role to play in ensuring technically that the warrant is implemented in keeping with the terms and conditions. Then, in terms of the information collected—as you say, actually reviewing it—that would be within the purview of the investigative team. A small number of people—you mentioned the monitors—monitors and analysts assigned to do the first review would be responsible to make sure that the condition is followed.

Then, of course, the—

Mr. Matthew Green: Just for my understanding, again, as we're trying to collect information for our own evidentiary process and the ability to send for papers and so on and so forth, on these 32 warrants, would there then be an audit or a report generated that would substantiate that that type of legal protection against the encroachment on the privacy of private citizens unrelated to the investigation would be protected?

Sgt Dave Cobey: I'm not aware of a report being produced for each case, but the ultimate accountability would come when the practices, the evidence collection practices, are challenged in court when these accused—

Mr. Matthew Green: That's not proactive. Surely, that's not the best-case scenario in internal policy to protect the privacy of Canadian citizens. Have you contemplated with this emergent technology proactive ways in which you can have your own internal checks and balances? Quite frankly, what we continue to hear from the government and from law enforcement agencies is to "take our word for it". I'm now asking you, given that you're responsible for reviewing the legality and the charter protections, and quite frankly, as I understand, the only party who has access to whether or not you're actually doing what is presented in the warrants, are there any reporting mechanisms that happen within your departments that would reflect the ongoing adherence to the warrants as they're being produced?

● (1645)

Sgt Dave Cobey: I'm not sure if you would be interested in hearing these steps, but I will say that we've implemented several proactive steps to make sure the warrants or ODITs are implemented effectively. Earlier in the process, we haven't specifically contemplated that report.

Mr. Matthew Green: Okay, thank you.

The Chair: All right, thank you.

With that, we will go to the second round.

First up is Mr. Kurek.

Go ahead.

Mr. Damien Kurek: Thank you very much, Mr. Chair, and to the members of the RCMP who are here. Thank you as well for the work you do to protect Canadians.

There are a few questions that I'm hoping to get as direct an answer as possible to. One, we've heard a lot about, though there's a little bit of discrepancy in, the number of authorizations, the number of individuals and the number of devices affected. That's not specifically the number I'm looking for here, but rather, the number of requests that have been made for judicial authorizations and were denied. Do you have that number available?

Sgt Dave Cobey: Do you mean judicial authorizations, or requests to use ODITs internally?

Mr. Damien Kurek: Both, if you could. I would like to get the number of requests internally to use the ODITs and any judicial authorizations that were denied, so I guess two different numbers.

Sgt Dave Cobey: The number of part VI authorizations denied is tracked in the annual federal wiretap surveillance report, so those numbers would be there. Do you want the other number as well?

Mr. Damien Kurek: Please.

Sgt Dave Cobey: Anecdotally, with regard to the number of investigators who request ODITs versus the number of investigations on which ODITs are deployed, I would say that one in 10 investigations that seek or are interested in using ODITs would actually make it through our process and have ODITs deployed. Because our process is quite rigorous and it's a very challenging practice to implement these tools, very few of the investigators who request them actually end up being able to use them.

Mr. Damien Kurek: When it comes to the use of ODITs—and it's obviously very complicated and we've talked a lot about the technological aspects of that—one of the challenges that exists and has been raised when using this sort of technology is solicitor-client privilege. Are there any examples where ODITs have been used where they have come into confrontation with attorney-client privilege and the use of this surveillance technology? Are there protocols in place to ensure that the rights of Canadians are protected in that regard?

Sgt Dave Cobey: The short answer is yes, there are protocols in place. The sample warrants you received, which is the sample part VI authorization, include specific terms and conditions related to solicitor-client privileges, and whether it be ODIT-collected information or information via a traditional telephone call, those terms and conditions must be followed.

Mr. Damien Kurek: There are a couple other questions I'd like to ask specifically related to both the testimony....

I've now served on this committee over the course of two Parliaments and there have been some very public disagreements between the leadership of the RCMP and the Office of the Privacy Commissioner, and, as was stated today, there's frustration that there seems to be a hesitancy on the part of the RCMP to disclose documentation to Parliament. Are you aware of the testimony that the Privacy Commissioner offered this morning? Would you agree that it was only after this information was made public at the end of June that the RCMP engaged specifically with the Office of the Privacy Commissioner related to ODITs' use in your investigations?

A/Commr Mark Flynn: I guess, again, that it goes back to the evolution of the technology, because in my history in the lawful access debate for 20 years now, the use of this type of technology and the challenges presented to the RCMP and policing in general from encryption have been a topic of discussion that involved the Privacy Commissioner, criminal law policy at DOJ and the human rights law section for many, many years.

Going back to a more recent time frame and the June date, I don't recall the exact order here, but I do know that technical operations did invite the Privacy Commissioner's office to the presentation that's occurring in August.

As well, you'll note some public articles that had been published by people such as Sergeant Dave Cobey here that are meant to bring more public visibility into what we are doing. We are pulling back the veil. We are trying to do that in a way that's professional, that respects both the law around the protection of tools and techniques—

● (1650)

Mr. Damien Kurek: If I could say, because I'm almost out of time, one of the concerns that I think has been highlighted by this committee is that it seems like only after details have been revealed—and this is not limited to this circumstance—is the RCMP up front about some of the details related to their investigation.

I would simply like to put one more thing on the record, and that's one important distinction. NSICOP is a committee of parliamentarians, not a standing committee of Parliament, and I think that's an important distinction that needs to be made.

The Chair: Thank you.

With that, you're out of time.

We'll go next to Ms. Hepfner for five minutes.

Ms. Lisa Hepfner: Thank you very much, Chair.

Thank you to the members of the RCMP here with us today.

I just want to start by asking: Why not do a privacy assessment every time the RCMP starts using some new technology? Why wouldn't a PIA be one of the first things you do?

A/Commr Mark Flynn: Going back to the point I raised earlier, it is a debate that we have, and sometimes it involves a discussion with the government advisory group and with the Privacy Commissioner's office as well, but we do take a look at what we are doing.

As I said, whether we're intercepting an analog communication or an encrypted communication, the privacy is in the content, not in the method of delivery. As we moved through time, we were looking at whether we were invading people's privacy any more. When it gets to a point where we believe there are concerns.... I've personally been involved in meetings where we've received advice that no PIA is required because we are not hitting the triggers. As an organization, we are changing our position on those, and I would say that, even in one particular case, we are moving ahead with the privacy impact assessment even though all of the advice that we have had is that one is not required.

We are trying to lean forward. We are moving forward. You have three people at this table today who believe strongly in erring on the side of revealing the details and allowing people to properly assess whether or not there is an additional invasion of privacy or whether or not we are simply doing things using a new method, but still substantially invading privacy at the same level as we previously had when authorized by judicial authority.

Ms. Lisa Hepfner: From your background information here, it looks like you would need.... Are there two warrants, a transmission data recorder warrant and a general warrant, to intercept computer functions and use ODITs? Would it be two warrants?

Do judges, in your opinion, really look at the privacy of unrelated people? Are judges concerned about Canadians' privacy when they're assessing these warrants?

Sgt Dave Cobey: To answer your question, there are more than two warrants. Predominantly, the omnibus order that we seek requires, in addition to a part VI, which is the interception of private communication warrant, a general warrant that is required for the deployment and use of the ODIT, the technology in the background. There's a transmission data recorder warrant that is required to collect the transmission data that we would collect to operate those, and then, if the ODIT is being used to collect information related to the location of the device, we also seek a tracking warrant. All of those warrants are included predominantly in the authorizations we seek.

Occasionally, we would seek only a general warrant if the objective were to only remotely search a device for historical information, but most of the time, we're using these tools for investigations that are ongoing and seeking prospective communications, private communications. So all of those warrants I listed, including a sealing order and an assistance order, are sought at the same time.

Ms. Lisa Hepfner: I think it was Mr. Flynn who talked about how similar technology was used as far back as 2012. I don't think we heard much detail about that technology and what was being done in 2012, so I'm wondering if I can give you a chance to expand on those comments.

● (1655)

A/Commr Mark Flynn: I'll add one element. I believe judges absolutely do understand privacy. That is their primary responsibility in weighing the needs of police to utilize such techniques.

Going back, in one of the previous questions the Delisle case was raised. If you look at the Delisle case, you will see in the news coverage that the RCMP, as part of our disclosure package, did present some of the material that was collected using the ODIT. This included screenshots of some of the communications between the accused in that case and what are believed to be the foreign actors he was engaged with.

When we speak about the technology, we hear “spyware”; we hear “malware”. I'll be frank. I don't believe it is either one of those. We are using tools and techniques that are designed to enable us to perform the duties that are expected to be performed by us in gathering evidence about criminal behaviour. You can see from the stats provided solely for 2017 onward that this involves serious cases with serious criminality.

Ms. Lisa Hepfner: Thank you very much.

I think that's my time, Chair, or do I have more time?

The Chair: No, we're just a little over, so we are done.

[*Translation*]

Go ahead, Mr. Villemure. You have two and a half minutes.

Mr. René Villemure: Thank you very much, Mr. Chair.

According to documents that were provided, the relevance of launching a public debate on the use of technologies was assessed in 2016. A public debate has not been held. There may be reasons for that, which you can explain to us.

Is there an openness to initiating a public debate on the use of intrusive technologies?

[*English*]

A/Commr Mark Flynn: Is there an openness to discuss the use of invasive...? I think the translation may have missed a fine point there.

I would say there's absolutely an interest in publicly discussing the use of invasive technologies. We're here. We're happy to have that discussion. Again, you'll see the news articles that cover it, so I won't waste your time.

[*Translation*]

Mr. René Villemure: You've been in your position since 2017.

Is that correct?

[*English*]

A/Commr Mark Flynn: I've been involved in this type of technology since 2002. I moved into a different position in 2015, and now I've been in my position in national security and protective policing since December, a year and a half ago.

[*Translation*]

Mr. René Villemure: Okay.

I'm still referring to the RCMP's desire to launch a public debate in 2016.

Is anyone able to tell me why this didn't occur?

[*English*]

D/Commr Bryan Larkin: I'm not sure any of us can respond to why it didn't occur in 2016. If we're very candid, Mr. Villemure, none of us were involved or actually participating in that process at the time, so—

[*Translation*]

Mr. René Villemure: If you ever find the answer, you can send it to us in writing. These are RCMP documents that I'm quoting.

As Mr. Green mentioned, we're talking about trust. We're not trying to carry out a witch hunt. The idea is to help you do your job in the best possible conditions.

Would you be open to having a third party audit or a third party assist you so that we don't have to believe you?

[*English*]

Sgt Dave Cobey: I would say the short answer is yes. Our involvement with senior federal and provincial prosecutors to make sure we get it right in terms of sharing enough detail with judges is an example of where we've reached out to third parties to try to get it right.

[*Translation*]

Mr. René Villemure: Okay.

Thank you very much.

[*English*]

The Chair: Thank you.

For two and a half minutes, we have Mr. Green.

Mr. Matthew Green: Thank you.

In the committee's latest study on facial recognition technology, the RCMP representatives told the committee about a new national strategy, the national technologies onboarding program. It's supposed to ensure that new technologies are assessed before they're used.

Why not just bring the Privacy Commissioner in there in an official way?

D/Commr Bryan Larkin: Thanks very much, Mr. Green.

I think one of our processes when we meet on August 23 will be to discuss how we modernize and evolve NTOP. That looks at all technology, centralized technology, so we have regulation, monitoring and good audits, and it also embeds GBA+ and legal assessments, etc.

That is a recommendation we're very much open to and something we look forward to.

Mr. Matthew Green: Given that the RCMP is currently subject to the Privacy Act, what practices are currently in place, perhaps referencing this new onboarding program, to ensure the RCMP's use of device investigation tools complies with the Privacy Act?

Sgt Dave Cobey: If I may, can I just respond briefly to your previous question?

● (1700)

Mr. Matthew Green: Sure.

Sgt Dave Cobey: In terms of NTOP and the OPC's being involved, I'm not sure of the status of it, but we actually did request whether the OPC would have an interest in embedding somebody in our program.

Mr. Matthew Green: When would that have happened?

Sgt Dave Cobey: It would have happened shortly after the report was released.

Mr. Matthew Green: Again, this kind of speaks to the reactionary way and the culture within the RCMP, quite frankly, that I've observed, after the fact.

With that being said, I still have a bit of a gap in what happens when the monitoring happens that might breach that fine line of here's our target, and our target is now around people not under investigation. Would that process also be open to a review basis? You know, with 32 occurrences that we know of going back to 2017, it feels like the Privacy Commissioner could have a meaningful role to play so that we at this committee don't have to embark on finding out after the fact in the media, quite frankly, which is a bit problematic.

Sgt Dave Cobey: I can tell you that as someone at the working level who's working every day with investigators and tech specialists to get this right, yes, we'd be happy to have more engagement from third parties like the OPC.

Mr. Matthew Green: Thank you.

The Chair: Thank you.

We'll go to Mr. Williams for five minutes.

Mr. Ryan Williams: Thank you very much, Mr. Chair.

Thank you again, gentlemen, for attending today.

I think the biggest balance we're looking for here is the balance between national security or your investigative work, which is very important, and then ensuring that we have public disclosure and protection of privacy laws as a whole. We know that's very difficult sometimes. I think as our colleagues have indicated, part of the reason we're here is that it was based on parliamentary work that was just asking certain questions in Parliament. It was a shock or a surprise to parliamentarians to find out that something was being used and no one knew anything about it—including who we would trust would be the Privacy Commissioner. Hearing today that technology's been used for 10 years....

As my colleagues have stated, we had investigations on other technologies, such as facial recognition technology, and from that we also found that the RCMP were not totally engaged with the process. We found that there wasn't that communication. Knowing that, and knowing that the one tool that the Privacy Commissioner has asked for, which is going to be implemented here in August....

I guess from a general standpoint, just so I can understand, why was the Privacy Commissioner not engaged even three years ago, when this was really being used in the judicial system in different processes? What is the best answer about why the Privacy Commissioner, who has, as he explained to us this morning, complete and airtight systems that keep everything confidential better than we can in an open committee in the public today...? Why was that not the first step taken with the RCMP?

A/Commr Mark Flynn: I can speak back even further than the last 10 years. I can go back more than a decade to almost two decades ago. Again, in terms of looking at what is the actual privacy invasion, we're focusing a lot on the tool and the methodology, but the privacy invasion is listening to the conversation and seeing what people are physically doing. We've installed for years; I've gone through the full Special "I" training program that is to install listening devices, hardware devices and cameras hidden discreetly in a particular location where criminal behaviour is occurring. This is a new method of invading privacy but invading privacy at the same level that it had been previously, whether it be through using those other techniques or through covert entry where you then extract all the data off of a computer—again, adhering to the terms and conditions of the court order.

So when you ask us when—about when we get to the point that we are actually seeing a level of privacy invasion that's different from what we have done before—that's really where the triggers come in for us. For those of us who have lived and done this work for two decades, you are seeing a slow evolution. There are times when we do need the checks and balances that come in and say that it's time to reflect and have new people come in. People like Sergeant Dave Cobey have come in. He is a strong advocate of being more public about what we're doing. He writes articles for the different journals and newspapers, etc., to try to bring visibility to this. That's really what the trigger is.

Mr. Ryan Williams: I 100% agree with that, but at the same time, we're here today, and what we talk about is the word "trust". We're trying to create and maintain 100% trust with government institutions and RCMP. Would it not have made sense—to counter your argument—that the Privacy Commissioner would have been the first one who would have been engaged in that process to ensure there's 100% trust and accountability?

● (1705)

A/Commr Mark Flynn: As I stated earlier as well, I am aware that the Privacy Commissioner's office, previous privacy commissioners, Department of Justice criminal law policy, human law section, have been involved in the lawful access debate that speaks to the reason behind the use of this technology and others for two decades. I know all of you are well aware of the lawful access debate and the multi-generational aspects to it.

I know those conversations have occurred at some levels. What made it to the Privacy Commissioners themselves I don't know. I do know we have had discussions. I can relay to you one in particular where we had a very fruitful conversation with the Privacy Commissioner's office around lawful access. We felt there was a strong understanding, and later on we received some contrary messaging. We've been involved in this debate. We welcome the transparency. We are open to it. We like the work that's been happening.

Mr. Ryan Williams: I think part of this committee's work, or the whole work, is to have recommendations because we're also modernizing our Privacy Act as a whole, not only to catch up to Europe and the Americans, but also probably trying as Canadians to get ahead of them.

What I'm going to ask for, in writing, is recommendations from your end, not just from our end, on what we can see to have more transparency and to modernize our Privacy Act the best we can, including protecting the confidentiality that you need to ensure that this kind of thing doesn't happen again. I think the biggest part that we're trying to talk about is that we have trust, trust in our government institutions. We've stated this over and over. I think that's where we're coming from. We want to see that. What recommendations can you give us that make sure that is maximized?

The Chair: Thank you.

I'm not sure that was really a question, but even if it was, we don't have time for an answer.

Mr. Ryan Williams: I'd like it in written format, if I can, through you, Mr. Chair.

The Chair: I think there was more of a request for a written response there. We'll take it as requested that way and move on now to Mrs. Valdez for five minutes.

Mrs. Rechie Valdez: Thank you to the RCMP for joining us for this study.

Mr. Chair, through you I'll be directing my questions to Sergeant Cobey. Anyone else can jump in to add additional comments if needed.

Sergeant Cobey, can you give us some detail on what criteria are used by the RCMP to determine whether these on-device investigative tools are used?

Sgt Dave Cobey: I can.

The most helpful way for me to explain those criteria that are used is to take you briefly through our process.

Initially we have a consultation with investigators who are considering these tools. During that consultation we explain to them—we demystify these tools and explain—just how complicated they are and the fact that they aren't necessarily going to be able to deliver the evidence they want, and we really encourage them to consider other, less invasive tools if possible.

Step one, we make sure they really understand what they're getting themselves into and have the resources to do it. Following that consultation, they have to submit an official request from their chain of command to our technical investigative services so there is executive awareness and oversight of their request to make sure it's been properly monitored.

After that request, and if it's approved on our side, then we have a second consultation involving their Crown prosecutor. Or, if they don't have a Crown prosecutor, we insist that a Crown be assigned so that a Crown understands the risks and the potential rewards of using these tools.

One thing we make clear during that consultation is that these are new technologies and we fully expect they will be litigated. We make sure they understand the litigation risk and the types of sensitive information that we're not able to share and would seek to protect under section 37 or section 38 of the Canada Evidence Act.

That whole process to date is really intended to make sure they understand that if there's another tool that works, they should use it, because these tools are complicated. Again, there's no guarantee they're going to work.

After all of those consultations, we do an engagement memo between our unit and the requesting unit to memorialize all the conversations, to set out the need to protect the tools. Only after that engagement memo is acknowledged by the commissioned officer overseeing that investigation would the assistance be provided. Of course, all that doesn't matter a whit unless judicial authorization has been granted through the process that we've described earlier in terms of a Crown agent, a proper authorization with all the terms and conditions we've included.

I hope that answers your question.

● (1710)

Mrs. Rechie Valdez: It does.

What kind of information can be obtained through ODIT searches that can't be obtained through a simple search warrant?

Sgt Dave Cobey: Well, typically ODITs are being sought during the investigation, so the objective of the ODIT, of course, is to collect the information while the target is still using it. Conducting a search warrant on a device necessitates taking the device away from the person, so obviously there will be an end to that person's use of the device. The information that can be collected is information that the suspect is still using or saving on that device before we've seized it, or before they know that they're the target of a police investigation.

Mrs. Rechie Valdez: Thank you.

Former prime minister Stephen Harper has been deeply involved with the Israeli start-up company Corsight AI, whose technology helps to identify facial recognition features in situations where they are difficult to identify.

Are you aware of the RCMP using any of this software technology?

Sgt Dave Cobey: I personally am not aware of that particular tool.

Mrs. Rechie Valdez: My understanding is that members of the opposition have indicated that the RCMP conducted mass surveillance of the population and, actually, members of Parliament. Do you have any comments on that?

Sgt Dave Cobey: I would go back to the earlier comment that these tools are never used to conduct mass surveillance. Again, judicial authorization is only granted by a judge if it's necessary and if the judge is satisfied that a particular offence involving a particular person and particular devices, and the way those devices are going to be intercepted, have been set out. It is very targeted. It is never mass surveillance.

Mrs. Rechie Valdez: Can you describe the challenge that you face in conducting search warrants and how this technology can better assist the RCMP in collecting key evidence?

Sgt Dave Cobey: I'll start with the second part of the question first.

I think this technology can assist in collecting valuable evidence because like every one of us in the room, criminal suspects carry devices. I suspect every one of us in this room uses a device in a way that is more complex for law enforcement, with the apps we use and the way we use our devices. None of that is conducive to the old-fashioned wiretap activities that enabled us to simply send our order to a telco and have them send us the communications.

Given all of the devices and the fact that users have complete choice over what device they buy, what apps they use and how they use those apps, ODITs are essential because they help us manage all that complexity.

The Chair: All right. Thank you.

Mrs. Rechie Valdez: Thank you.

The Chair: That takes us through the first two complete rounds, per the motion adopted by committee. I am going to deviate from that just because time is becoming a factor.

For the third round, we'll go to four minutes each for Mr. Bezan and Mr. Bains, two minutes each for Mr. Villemure and Mr. Green and then four minutes each for Mr. Kurek and Ms. Khalid. That will get us just about jammed into ending on time, or maybe a minute or two over.

With that, go ahead, Mr. Bezan, for four minutes.

Mr. James Bezan: Thank you. It's been an interesting discussion.

When you go for a warrant, does the RCMP need to notify the service carrier that somebody who has one of their devices—Rogers, Telus, Bell—has a system being hacked with RCMP spyware? Is there any duty to disclose?

Sgt Dave Cobey: I wouldn't characterize our activities the way you have, but I would say the service providers are not involved when we use ODITs.

Mr. James Bezan: Okay, so again, when you're monitoring conversations, using the microphone and hacking in to look at chats and emails, what about the other parties, the third parties who are innocent bystanders, such as friends, relatives and spouses, for example? How do you protect their privacy?

Sgt Dave Cobey: It's a great question. Protecting innocent third persons' privacy and non-pertinent communications has been an issue ever since wiretapping began. If you look at the sample order that we provided, there are terms and conditions in there. Setting aside the ODIT for a moment, there are terms and conditions for regular wiretapping. Again, we'll go back to privileged communications. Privileged communications between a solicitor and their client have to be protected and treated in a very special way. The same applies to ODIT collections, and some of the terms and conditions in that sample order, which is representative of the orders that we seek, include the fact that non-pertinent information related to third parties and others has to be set aside, protected and only dealt with as guided by the court.

Another specific example, which is also included in that order, is the requirement that the hot mike feature described in the technical document can only be activated if there are grounds to believe that one of the principal known persons, as we call them, the—

● (1715)

Mr. James Bezan: In a case where you have solicitor-client privilege and you're monitoring an individual, and they're meeting with their lawyer, and they say, “By the way, not only are we laundering money, but we also have a drug shipment coming in through the port”, you wouldn't act upon that information?

Sgt Dave Cobey: If a person is involved in a communication with their solicitor, the terms and conditions are clear. They have to be sealed, and we can't look at those without a further order of the court.

Mr. James Bezan: Mr. Flynn, just quickly, you were talking about how you've been around for a long time on this file. Can you talk to the memorandum of understanding that the RCMP has with CSIS and with CSE in particular? As the Communications Security Establishment, they have a lot of spyware that they have been using internationally on non-Canadians. What type of relationship does RCMP have with CSE?

A/Commr Mark Flynn: Speaking broadly, as the question was, the RCMP, from a national security perspective, works in partnership with all of the national security agencies, which obviously include CSIS, CSE and CBSA. I could go on with a long list of national security partners.

Specifically, with respect to our relationship with CSE, CSE does have a mandate C provision for providing us technical assistance through technical operations where tech ops manages that relationship with CSE, but I can say that, in that relationship, it does not expand the authorities of the RCMP.

Mr. James Bezan: Thank you.

Mr. Chair, because we requested information and never got it, I'd like to move the following motion:

> That, pursuant to the motion adopted by the committee on July 26, 2022, the committee re-affirm its request for all the documents outlined in its original motion. That any documents received from the RCMP that include warrants, lists of warrants, the scope of warrants and the affidavits submitted in support of the warrant applications be considered by the committee in camera only, and following the parameters outlined below:
>
> That all documents issued pursuant to this motion be provided to the Office of the Law Clerk and Parliamentary Counsel within 15 days of the adoption of this order,
>
> That all relevant documents be vetted for matters of personal privacy information, ongoing police operations, and national security by the Law Clerk and Parliamentary Counsel within seven days of the receipt of the documents,
>
> That all documents be circulated to committee members, at the earliest opportunity, once vetted.

I'll speak to that motion, Mr. Chair, because I want to assure committee members and the RCMP that we don't want to undermine any investigations they have right now that are looking at criminality or national security.

What we do want to see is just the broad scope of what those warrants look like and the documents that are associated with them. Through the vetting process that we've used in the past at a number of parliamentary committees, the Law Clerk and Parliamentary Counsel would ensure that the documents are redacted and that the information that's withheld from us as committee members falls in line with protecting those investigations, national security and the privacy of those individuals who are subjects of interest.

I've forwarded this to the clerk, and I've asked that it be circulated. All committee members should have the motion before them now. I just received it myself. It's in both official languages.

The Chair: It is in order.

Before we do anything else or return, with the limited time we have left, to rounds of questions, we go to debate.

I have Ms. Khalid.

Ms. Iqra Khalid: Thanks, Chair.

I would respectfully submit to members.... Obviously, I haven't had the chance to review it, but we do have the RCMP here for another 11 minutes. I suggest that perhaps we go to our witnesses and then, having reviewed this motion, deal with it as the first order of business at tomorrow's meeting.

● (1720)

The Chair: I guess that's a suggestion. I can canvass the room.

Is there interest in—

Mr. James Bezan: Mr. Chair, I'd just say this.

I think that we should.... Based upon the lack of information that was provided by the RCMP.... I appreciate what they've given us. They gave us some background information, but it doesn't talk to the broader scope of the motion that we brought forward. In respect of the parliamentary process—

The Chair: I was merely just—

Mr. James Bezan: I'll just say this. We should deal with this motion because tomorrow we have a full slate, and I'd like to get to witnesses tomorrow rather than spending all day debating this motion.

The Chair: We do indeed.

I have Mr. Fergus with his hand up as well. Do I see anybody else in the room?

Mr. Fergus is the only one I see right now.

Go ahead, Mr. Fergus.

[*Translation*]

Hon. Greg Fergus (Hull—Aylmer, Lib.): I wanted to say exactly the same thing as Ms. Khalid. For me, it's very late. I'd like to know if we can read the motion and continue with the witnesses who are here. That can be the first thing we deal with tomorrow.

[*English*]

The Chair: All right. Procedurally, I'm not....

I'm going to just spend one moment to have a quick word with the clerk.

Okay, we really are running out of time to do both—have additional questions of our witnesses and still allow time if members want to consider this motion—so I guess unless there's an actual motion to adjourn or suspend the debate, there really isn't any way for me to deal with this.

I see that Ms. Khalid has her hand up again, and so does Mr. Fergus.

Go ahead, Ms. Khalid.

Ms. Iqra Khalid: Thank you, Mr. Chair.

I just want to reiterate because, based on what we heard today from the RCMP, from the OPC and from the minister, I feel that there may be other documents that we might want to add to this list. For example, we heard that there was some activity in 2012 that we may want to pursue. That's why I was hoping that we would have some time to perhaps go back, review the testimony, and see how else we can strengthen this motion—what other documents—rather than keep on doing it again and again and again in a piecemeal kind of way. We could do it in a more substantial and fulsome kind of way.

I am, myself, quite interested in the 2012 reference that was made. I know that some members might be interested in other things that perhaps we could include with the text of this motion, perhaps. I just wonder if there are members who would be willing to just give it a little bit of time to see if we can really expand this out.

The Chair: Thank you.

Mr. Fergus.

[*Translation*]

Hon. Greg Fergus: Thank you, Mr. Chair.

If you want me to put forward a motion to adjourn the debate, I'd be pleased to do so.

I wanted to know if we can come to an agreement among colleagues. As I said, I would like us to take this up tomorrow morning at the beginning of the meeting, at 11 a.m. That would give us time to read the documents and take into consideration what Ms. Khalid suggested.

Perhaps there's a way to improve the motion. Give us a few hours to read through these documents so we can propose amendments. Then we can have a great debate. I think that would be the best way to go, but I'd like to know if we can—

● (1725)

[*English*]

The Chair: I'm going to have to interrupt you, Mr. Fergus. If you are, in fact, moving to adjourn debate, that's dilatory and non-debatable and ought to be voted on. In terms of just doing this without a vote, I'm seeing some furrowed brows and shaking heads in the room, so I don't know that this could be done other than by way of a vote.

If you have moved, Mr. Fergus, to adjourn debate, then I'm going to have to call a vote.

[*Translation*]

Hon. Greg Fergus: Can you hear me okay?

[*English*]

The Chair: I can hear you in translation, but you're not very loud in the room.

Hon. Greg Fergus: Oh, so, you can't hear me in English?

The Chair: I can hear you in English now. You're okay now.

Hon. Greg Fergus: All right.

Mr. Chair, I don't have the pleasure of being in the room. Actually, I have the great pleasure of not being in the room, given where I am. Is there no appetite for us to just have this debate first thing tomorrow morning?

The Chair: Am I sensing in the room that there is an appetite to adjourn debate?

Mr. James Bezan: He moves to adjourn. Deal with it.

The Chair: No, there is no consensus, anyway, to leave this until the morning. There are members who are very keen on the witnesses. We have a full slate of witnesses.

I would offer the opportunity.... We went two hours. Only for tomorrow, I think we have built into our availability some time for committee business if we extend one of the meetings tomorrow. Is that a possibility?

Hon. Greg Fergus: That works for me.

The Chair: Okay. This is my proposal. Following the time allowed for witnesses tomorrow—I'll maybe make it in the first panel, just in case people are travelling after the second panel—we'll have some time for committee business where we can consider both the motion that Mr. Bezan has made and any possible amendments that may expand the motion, which Ms. Khalid had in mind.

Is that reasonable? I'm just looking for a co-operative solution here.

Mr. James Bezan: I think that, procedurally, you have a motion on the floor, and you need to have debate or a motion to adjourn debate.

The Chair: Indeed you're right. We have a motion on the floor that could be voted on right now if there is no debate. I see Ms. Khalid has her hand up. We're at about 20 minutes after 5. I can't let this go too much over 5:30 with the House resources available.

Go ahead, Ms. Khalid.

Ms. Iqra Khalid: Thank you, Chair.

To speak to the motion itself, I'm sure Mr. Bezan took some time to draft it. I'm sure he conferred with his colleagues who are in the room.

Again, I said this earlier today as well. I will reiterate that if you had circulated the text of the motion to me, to any of our Liberal members with a little bit of notice, we would have been able to review the document. We would have been able to have a substantive conversation.

We have two minutes left in a committee meeting, and we are now being forced to vote on something that we haven't even reviewed. We haven't had the opportunity to have a conversation about this. We haven't been given the courtesy by members in this room to say, “Hey, look, this is what we're proposing. Let's do this. Let's get this done.”

We're here. We're willing. We're asking questions. We're taking an interest in this very important study. We would just hope that we could be more collaborative.

I absolutely agree with the chair. I feel that with just a click of a button you could have flipped me an email. You could have given me a text or what have you. We would have been able to have a conversation on the side or simultaneously as the committee hearing was ongoing. Now, all of a sudden, we're facing a place where I haven't read the full text of the motion. Yes, it's on my phone here in front of me. I haven't read it. I haven't contemplated what else, what scope. I haven't had the time to digest what I've heard from the RCMP today to see where that lack is.

I would like us to be a little bit more collaborative, Mr. Chair. It is very unfortunate that we're having to complain to you about this lack of co-operation. I understand that you all have the votes. You're good to pass your motion in whatever way you want.

I'd just ask for a little bit of respect for the committee's time, for everybody's time here, just to be more co-operative, more collaborative, and for us to get things together without being so confrontational all the time, folks. We're here to work together with all of you guys.

● (1730)

The Chair: Thank you.

Mr. Fergus.

Hon. Greg Fergus: Thank you, Mr. Chair.

It really comes down to that. Look, folks, this is an opportunity. I think we're all on the same page here. I think we all are keenly interested in this issue. We all want to have a fulsome debate. I think there's an opportunity for us to do this.

Let's be frank. We don't have a full roster of witnesses tomorrow. I think the chair's suggestion was very co-operative, and one that I think everyone can support. We have time tomorrow so that we can do this without cutting back on witnesses, so why not? It's only a couple of hours later, folks.

The Chair: All right, I have Monsieur Villemure.

[*Translation*]

Mr. René Villemure: Would it be possible to ensure that everyone has the right equipment tomorrow? We need to be able to hear what people are saying. Unfortunately, there are times when I can't hear Mr. Fergus, which is unfortunate because I like to hear what he has to say.

Thank you.

[*English*]

The Chair: You are correct, Monsieur Villemure, we have had a little bit of audio trouble from time to time. Mr. Fergus was cutting in and out a little and was hard to hear at some moments. I'm not sure what we can do about that other than to ensure that there's awareness.

I have both.... I don't know who's first. I think it's Ms. Khalid first. We just had Greg, so go ahead, Iqra.

Ms. Iqra Khalid: Thanks, Chair.

In the interest of the plan that you presented, which I find to be a reasonable one, I move that the debate be adjourned until tomorrow on this motion.

The Chair: The motion with the condition added there becomes debatable, so is there anybody who wishes to speak to the motion?

Iqra, you could remove the condition and say simply that debate be adjourned on the motion. Okay, adjourned until tomorrow.

There is no debate, so if it's okay either way, then we'll go to the vote.

Ms. Iqra Khalid: Sorry, Chair, I believe Mr. Fergus' hand has been up.

The Chair: Okay, I think his camera disengaged, and then when that happens I no longer see his hand.

Go ahead, Mr. Fergus.

Hon. Greg Fergus: My apologies, I was going back to reading the motion on my P9 email account.

[*Translation*]

I would like to apologize to all members, particularly my colleague from the Bloc Québécois. The reason I don't have the headset is because the meeting was called while I was out of the country, and I didn't have my headset or my computer with me. I'm sorry about that.

Again, I apologize to all my colleagues and to the interpreters.

[*English*]

The Chair: All right, we're at this point.... If there's no other debate then we can vote on Iqra's motion, which is to adjourn debate.

(Motion agreed to)

The Chair: With that, we are past our time. The meeting is adjourned.