HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

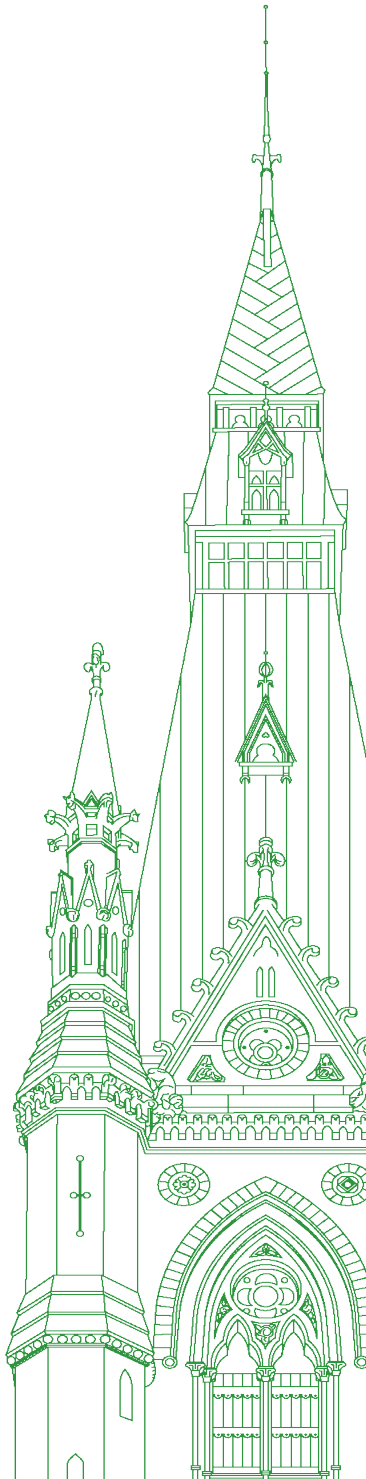
44th PARLIAMENT, 1st SESSION

Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 032

Tuesday, August 9, 2022



Chair: Mr. Pat Kelly

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, August 9, 2022

● (1105)

[*English*]

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

Welcome, everyone, to meeting number 32 of the Standing Committee on Access to Information, Privacy and Ethics. Pursuant to Standing Order 108(3)(h) 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.

I've just discovered in the notice that this morning we have two witnesses for this meeting. I am going to run the meeting in two separate panels. These are the witnesses who were contained in the motion we adopted. In our meeting this afternoon, we will have, in one panel, all three of the witnesses who were provided by the parties.

We'll begin with Mr. Therrien for the first hour, and then in the second hour we will have Ms. Polsky.

With that, I welcome former commissioner Therrien, who is no stranger to our committee. We've had many committee meetings together. I welcome him back and invite him to begin this first panel with his opening statement.

Mr. Therrien, you have up to five minutes.

[*Translation*]

Mr. Daniel Therrien (Lawyer, As an Individual): Thank you very much, Mr. Chair.

It's a pleasure to be here.

Thank you for inviting me to testify as part of the important study you are conducting further to the June 22 publication of the government's response to a question that MP Tako Van Popta asked regarding mobile device surveillance.

In that response, the Royal Canadian Mounted Police, the RCMP, revealed that it had secretly used device investigation tools to collect data from mobile and other electronic devices of Canadians, always with judicial authorization pursuant to the Criminal Code.

[*English*]

I have no knowledge of facts beyond what was reported by the RCMP in response to Mr. Van Popta. My remarks, therefore, will focus on the content of the applicable law. I know that the RCMP reiterated yesterday that it does not use what it calls ODITs without judicial authorization as this would be an offence under the Criminal Code.

There is no doubt that the covert collection by the state of personal and other information residing on the digital devices of Canadians is an extremely intrusive practice. However, such level of intrusiveness can still be lawful and consistent with privacy principles if the collection of information is authorized by law and is necessary and proportional to the achievement of compelling government objectives.

The RCMP says that its use of on-device investigative tools always follows judicial authorization, pursuant to the Criminal Code. These provisions include several privacy safeguards. They can be invoked only for serious crimes. They require judicial authorization, often on a high standard of reasonable grounds to believe that a crime has been or will be committed and that evidence related to the crime will be found on the device to be searched. Judges can subject the collection of information to terms and conditions, including conditions designed to limit the invasion of privacy.

[*Translation*]

I believe that these provisions are reasonable or, at least, that they constitute a good starting point for protecting privacy in the context of criminal investigations in which the state has compelling grounds to act and in which its actions are governed by judicial authorization.

Can those provisions be improved? Possibly, and the government seems receptive to the idea. However, to conclude that statutory changes are necessary, I think it would be important to determine how the current provisions have been applied and, where possible, to identify grounds for concern. You questioned the RCMP about this, particularly regarding the content of warrants obtained.

Your study ultimately concerns the fundamental conditions that must exist so that Canadians can be confident that their rights are protected when law enforcement agencies employ intrusive methods. And central to that issue of confidence is the existence of a sound legal framework and independent oversight. The balance between the transparency and protection of police methods is also an issue. I will be pleased to address those themes at greater length in response to your questions.

Lastly, the RCMP supports the use of device investigation tools and other intrusive methods in addressing the issues raised by data encryption, for example. I think that's acceptable provided the use of those methods is subject to judicial authorization on a case-by-case basis and the protection that encryption affords the general public is not otherwise compromised. On that point, I refer you to the brief published by the Office of the Privacy Commissioner on December 5, 2016, as part of a government consultation on Canada's national security framework.

I will be pleased to answer your questions.

[*English*]

The Chair: Thank you, Mr. Therrien.

Before I go to the first speaker, I have some housekeeping information for committee members. We not only potentially have to deal with motions that may be moved, but we also have to give some instructions to the analysts. I propose that we do that at the end of the second panel. I'm told by the clerk that we will have a few minutes at the end of the second panel to deal with those items of committee business, so that's my intention.

With that, the first round of questions will begin with Mr. Bezan.

You have up to six minutes.

● (1110)

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

I want to thank you, Mr. Therrien, for joining us today.

What years did you serve as the Privacy Commissioner of Canada?

Mr. Daniel Therrien: I served between 2014 and 2022.

Mr. James Bezan: Were you surprised, during the testimony yesterday by the RCMP and Minister Mendicino, that the on-device investigative tool for hacking into our cellphones predated your time as Privacy Commissioner and they never once consulted you or asked about the privacy impact of using this on our devices?

Mr. Daniel Therrien: I was surprised by the tool itself, by how intrusive it is, and that it was used for so long. Certainly, there have been many discussions over the years—as the RCMP said yesterday, probably since the early 2000s—on the lawful access issue. Both in my term as commissioner and when I was at the Department of Justice, I was following and part of these discussions. But the use of this particular tool to go around encryption, yes, was a surprise.

Mr. James Bezan: When you look at their, I guess, intentional non-disclosure of using this technology, if you'd known about it sooner, would there have been recommendations made on how it should be used to protect the privacy of Canadians, coming from the Office of the Privacy Commissioner? Had you known, would you have been more, I guess, condemning of the RCMP for the use of this technology, or of Public Safety, for that matter, for not providing the regulatory tools to ensure the protection of the privacy of Canadians?

Mr. Daniel Therrien: It's a complicated question. I would say, as Commissioner Dufresne said yesterday, that I would have looked at—as he will—the detailed conditions under which this tool would be used to see whether there were any recommendations to be made on how it would be used beyond the four corners of the law, which is, again, a good start.

Part VI of the Criminal Code is a good start. It sets privacy safeguards. It sets high thresholds for judicial authorization. It has judicial authorization, so it's not as though the RCMP can use this tool without oversight by an independent body. But even with all of these good safeguards, I would have looked at—and I understand that Mr. Dufresne will—the sum total of the conditions under which the tool is used to see whether any further recommendations could be made on how to use it in a way that protects privacy.

Mr. James Bezan: As you know, as somebody with a great deal of experience on legal matters and the workings of government and providing advice on things like justice and protecting the rights of individuals, under section VI of the Criminal Code there are different types of warrants, whether it's a wiretap or video surveillance. There are general warrants that are more broad-sweeping. Do we need to have a recommendation for a new type of warrant for the use of on-device investigative technology?

Mr. Daniel Therrien: You asked yesterday whether judges who receive requests for judicial authorization have the technical.... They certainly have the legal expertise, or they have the technical expertise to make the best decisions, I'm assuming. I heard yesterday in testimony from the government—I think from the minister and certainly from the RCMP—that judges of superior courts have the expertise, so there must be some training given to judges.

Should there be special kinds of warrants? It would depend on whether the current regime as applied by judges with the expertise, legal and technical, they have, is sufficient to protect privacy. It may well be. I don't know.

● (1115)

Mr. James Bezan: Yesterday we were talking about the Order Paper question. The Order Paper question actually said the RCMP had consulted with you as Privacy Commissioner, or with the Office of the Privacy Commissioner, about the use of ODITs, which we now know never happened. How did you interpret that response to the Order Paper question versus their actual testimony?

Mr. Daniel Therrien: The comment that we were consulted most likely related to some other related initiative, not the use of this particular technology.

Mr. James Bezan: As we look at zero-click spyware like Pegasus, now we're finding out there are other companies out there—

The Chair: Mr. Bezan, you really are out of time.

Mr. James Bezan: Okay.

The Chair: Wind it up quickly.

Mr. James Bezan: Thank you. Are you sure that was six minutes?

The Chair: Yes. You started asking a question at five minutes and 55 seconds.

We're going to Ms. Hepfner for up to six minutes.

Ms. Lisa Hepfner (Hamilton Mountain, Lib.): Thank you, Chair.

Thank you, Mr. Therrien, for being with us again today.

You mentioned during your opening statement that you understand that even technology as intrusive as an ODIT can be lawful in some circumstances. It can be necessary for law enforcement to have the ability to be that intrusive.

Could you go into more detail about what sorts of situations might require police to have a tool like this?

Mr. Daniel Therrien: I think what's at play is the balancing of privacy and other public interests. There is no question that this particular tool is extremely intrusive. It's more intrusive than traditional wiretap tools. It does not just record communications on the phone between person A and person B. It sits on the phone, on the digital device of the individual, and the state—the police—has access to everything on that phone. It is extremely intrusive.

When you look at the balancing, therefore, there needs to be an extremely compelling public interest to justify the state being able to have that kind of information and use these tools. The Criminal Code sets out a limited list of offences, serious offences, where the police, with judicial authorization, are able to use the technology in question—things like murder, terrorism, drug trafficking and the like.

I think by and large the list of offences in question does fit the definition of "compelling state imperatives".

Ms. Lisa Hepfner: Given that technology has advanced so much and that criminal organizations are very easily able to overcome traditional types of wiretapping, I'm wondering why you were surprised to know that police had advanced their abilities to investigate in the current technological age.

Mr. Daniel Therrien: My surprise did not relate to the fact that the police have technologies to intercept communications in the context of investigations. Traditionally these tools were somewhat limited. Wiretaps, again, intercept a specific communication. It is the intrusiveness of the tool that surprised me, not the fact that the state would use technology in the context of investigations.

Ms. Lisa Hepfner: What we heard from the police yesterday is that communications these days are encrypted either before they leave the device or when they come in. This is the technology they would use to overcome that encryption.

Mr. Daniel Therrien: I accept that. I accept that encryption, although it has many benefits for society protecting the privacy of communications of ordinary Canadians, commercial transactions and the like, can pose serious challenges for law enforcement. I accept that.

As I said in my opening statement, I think that to have technology to address the challenges of encryption with judicial authorization on a case-by-case basis does not impede others from benefiting from encryption. I think that's acceptable.

I'll say that part of my surprise was that there has been an ongoing public debate in the context of lawful access about this specific issue and to what extent the police can use means to overcome challenges of encryption, and it never came about in public debate that ODITs were used to that effect.

I'm not saying that it is unacceptable for ODITs to be used, but it was surprising that, in the context of many debates in the public about the challenges of encryption when I was Privacy Commissioner, I was not told that a tool was used to overcome encryption.

● (1120)

Ms. Lisa Hepfner: Is there any evidence or any indication that the RCMP has used this tool beyond the scope of what's allowed in the Criminal Code? Was there any indication of mass surveillance or anything like that?

Mr. Daniel Therrien: I don't have that. I know that the RCMP said yesterday that it's not just a question of just believing them. They told you yesterday that it would be a crime for them to use the tool without judicial authorization and that they do not do that. I accept that.

Ms. Lisa Hepfner: Thanks very much.

I'm pretty much out of time, Chair, so I'll cede the floor.

The Chair: We'll go to Mr. Villemure.

[*Translation*]

Mr. René Villemure (Trois-Rivières, BQ): Thank you, Mr. Chair.

Mr. Therrien, thank you for testifying before us once again.

We always appreciate your informed comments.

Yesterday, Commissioner Dufresne said he was surprised to learn the facts, and, unless I'm mistaken, I believe you were too.

The aim of our debate is to preserve the public's trust in our institutions. I believe the Office of the Privacy Commissioner of Canada is one of the leading institutions, one of the preferred institutions, in achieving that end.

RCMP representatives told us they had consulted you. In other studies, we also learned that you had been consulted but were unable to look under the hood, as it were. It seems to me the RCMP consults you on trivial matters so it can say it consulted you but refrains from doing so on other matters.

Am I wrong in saying so?

Mr. Daniel Therrien: I think that's a central issue in your study. It may be more complicated than it seems.

Yesterday, you discussed the possibility of amending the act to provide for the conduct of privacy impact assessments, PIAs. That's a legal obligation, and I think it's a very good idea. This obligation currently derives from a Treasury Board standard or policy. It's somewhat vague on when assessments are to be conducted and when the commissioner must be consulted.

Going back to what I said a little earlier, I repeat that the fundamental conditions for confidence are clear legal rules, high legal standards and independent oversight.

Part VI of the Criminal Code provides for all that. It's not as though there aren't any rules; there are rules. Can those rules be improved? Probably.

Yesterday, you discussed a potential improvement: that the RCMP or other federal institutions be required to consult the Office of the Privacy Commissioner and that they have a legal duty to do so. That's a good idea, but if you recommend that it should be a legal obligation, I encourage you to specify the circumstances in which assessments must be conducted. Under the Treasury Board standard, an assessment must be conducted where a new or deeply altered program has an impact on privacy. The RCMP told you yesterday that the fact that it uses this technology in particular is nothing new. You shouldn't focus on the technology, but rather on the violation of privacy. According to the RCMP, there are supporting arguments in this matter. I don't personally agree with that, but I don't think it's an unreasonable position.

I think that, in addition to saying there's a legal obligation to conduct assessments, you also have a responsibility to state in general terms when they must be conducted and for what purpose. That way you can ensure proactively that the act is being complied with. There wouldn't simply be an *ex post facto* review but also a preliminary examination to ensure statutory compliance. Ideally, you should also recognize privacy as a fundamental right, as Mr. Dufresne suggested yesterday.

● (1125)

Mr. René Villemure: Absolutely.

When was part VI of the act passed?

Mr. Daniel Therrien: Do you mean the statutory provisions on privacy?

Mr. René Villemure: Yes.

Mr. Daniel Therrien: The legislation dates back to the 1980s.

Mr. René Villemure: So it's reasonable to believe a review of the legislation might be in the cards.

Isn't it?

Mr. Daniel Therrien: Yes, that's the least you could say.

Mr. René Villemure: Yesterday, there was a lot of talk about part VI of the Criminal Code. You know as well as I do that a situation may be lawful but unethical for many reasons. It seems to me it's not enough to address part VI. We have to be able to examine the situation impartially. The impression I got yesterday was that I was being forced to believe the RCMP. We had to believe it.

Do we have to maintain that position, that we must believe the RCMP? If that's the case, does that preserve or increase public trust?

Mr. Daniel Therrien: I don't think the situation is the same as in the Clearview AI affair. In that case, the legal framework regarding facial recognition was weak, nearly nonexistent. There was also no oversight by an independent authority.

Part VI provides a legal framework comprising strict standards and independent oversight by the courts. Is that regime perfect and impossible to improve? The answer is no. We have a good starting point.

Mr. Daniel Therrien: As a result of that starting point, I believe the public should trust that the RCMP will not commit a crime by using this tool without judicial authorization, as its representatives asserted yesterday. However, it's no doubt possible to improve that legal framework proactively, particularly with regard to privacy impact assessments.

Mr. René Villemure: We have to continue.

Mr. René Villemure: Thank you very much.

[*English*]

The Chair: Thank you.

Now we'll move along to Mr. Green.

You have up to six minutes.

Mr. Matthew Green (Hamilton Centre, NDP): Thank you.

I'd like to continue on getting to the heart of the matter for me, which is about strengthening legal frameworks.

We heard from the Privacy Commissioner earlier in testimony the suggestion that privacy impact assessments should be part of the process. We heard from the deputy commissioner, at least in the documents that we received, that they have a process for onboarding new technology.

Given your past experience in this, and understanding that much of our work as an ethics committee has been chasing situations after the fact in a very reactionary way, what points of legal framework would you recommend to this committee to help close the gap that clearly exists with what is legal, ethical and technological in terms of the rate of advancement of the technology versus the existing legislation?

Mr. Daniel Therrien: If we start with the potential amendment that would make it a legal requirement as opposed to simply a policy for departments and institutions, including the RCMP, to proceed with privacy impact assessments, it's a good start.

On this point—and Commissioner Dufresne spoke about the role of the OPC here—I just suggested to Mr. Villemure that perhaps you want to make recommendations, not only on creating a legal requirement but on having a certain definition of what these PIAs are for. I would encourage you to consider the role of the OPC and the role of the courts.

I don't think the OPC should duplicate the role the courts play under part VI of the Criminal Code. I think the OPC's added value to the courts would be to look proactively at a program level, not at an individual case level, the conditions under which the tool would be used and make recommendations to that effect.

● (1130)

Mr. Matthew Green: I would tend to agree.

We heard as well, with the Privacy Act coming up, the distinction of language being included in the preamble versus the actual legal framework to provide guardrails.

In your experience, both with the Department of Justice and in the OPC, what recommendations would you provide in the upcoming Privacy Act that would be part of the legal framework that would provide, not just for law enforcement, but more broadly for the protection of this type of use against citizens here in Canada?

Mr. Daniel Therrien: I think a preamble is a good idea.

You said yesterday that you would want clear legal standards such as the requirement to proceed with a PIA, and I agree, but a preamble helps set for everyone, including government institutions, how we look at privacy when a privacy impact assessment is made. For a preamble to say that privacy is a fundamental right essential for the preservation of the dignity of individuals, when the RCMP, the health department or whatever institution proceeds with a PIA, they have that important message in mind. It's not a check box exercise—

Mr. Matthew Green: It was also determined that it's not legally binding. How would we make legally binding the entrenchment of those rights, as fundamental rights within the framework of the Privacy Act?

Mr. Daniel Therrien: The preamble can still be used as an interpretive tool. It's important to have a clear legal standard. Thou shalt proceed with a PIA—that's a clear legal standard, but a preamble, although not executory in itself, is a very helpful interpretive tool to give life to the legal standard in question.

Mr. Matthew Green: I'm going to follow a different line now. We've gone from the policy directives and hopefully the recommendations for legislation to what I believe to be an existing gap in oversight, which is what my colleagues have talked about—the police policing the police.

In the sample warrant that was provided, there was a section on interceptions by on-device investigative tools that talked about oral communications 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".

Essentially, we have the situation set up where this is placed on a device; it's being monitored and we're supposed to take their word for it even though, as described by the RCMP, they have no processes in place for auditing or performance evaluation of the sort. My concern is that, left unchecked, without explicit guardrails as to when and how this can be used, the comprehensive nature of the capture of data seems to be susceptible to unlawful search and seizure of subjects and materials outside of the purview of the warrant.

Do you have any comment on that and the ways we might be able to provide oversight?

Mr. Daniel Therrien: You might be partially surprised by my answer.

I don't think the RCMP is a rogue institution. Currently, they say, and I accept, that they use ODITs only with judicial authorization, and judicial authorization comes with terms and conditions. I do not start from the premise that the RCMP wishes to disrespect these terms and conditions. It may actually be a crime to disrespect the terms and conditions in question because the use of the tool is only lawful if consistent with the terms and conditions imposed by the court.

That said, it might be a good idea to have auditing processes to ensure that the police officer who has to perform the task in question does so in compliance with the court.

● (1135)

The Chair: I'm really loath to do so, but I must interrupt because we're significantly over time with that answer. If you didn't complete your thought, maybe we could incorporate that in another response.

Mr. Daniel Therrien: No, I completed my thought.

The Chair: It is time to go to Mr. Williams for up to five minutes.

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

Mr. Therrien, thank you very much for joining us today.

You were the Privacy Commissioner for eight years. Is that correct?

Mr. Daniel Therrien: Yes, I was.

Mr. Ryan Williams: In your words, why is the privacy commission an important part of the Canadian government?

Mr. Daniel Therrien: The OPC plays a number of roles. One of them is to investigate complaints and serve, as I said a few minutes ago, as an independent oversight to the government. The government has to comply with the law. It is assisted by the justice department, whose duty is to ensure that the government acts in accordance within the law, but all of these processes are within the executive branch.

One of the roles of the OPC is to provide confidence and trust to the population by having an independent look beyond the executive branch mechanisms to ensure that laws, and particularly privacy laws, are indeed being respected. It also has a proactive role.

Mr. Ryan Williams: Where I'm going with this, as I think you've mentioned, is that it's about trust.

Mr. Daniel Therrien: Yes.

Mr. Ryan Williams: It's about instilling trust in Canadians that when we have government and institutions acting in many different ways, they can trust those institutions. Would that be correct?

Mr. Daniel Therrien: Yes.

Mr. Ryan Williams: Yesterday, as I think you heard as well, we heard from the RCMP and the minister that judges are only giving warrants where needed, that this technology is safe and that we can trust them. They stated they didn't feel they needed to do these PIAs, privacy impact assessments, and we've seen that.

In your opinion, how right is that? Can we just trust government intrinsically? Can we just get rid of the privacy commission? How true are the words they're saying?

Mr. Daniel Therrien: With respect, I don't think that's an example of “trust us” when they say courts only give the authorizations after review and therefore this is lawful. You say, "trust us". The question of trust depends on two things: a clear and rigorous legal framework and independent oversight. The courts provide independent oversight.

We have a good starting point with part VI of the Criminal Code. Can it be improved? Probably.

The OPC certainly has particular expertise in privacy to bring to bear, and proceeding with privacy impact assessments is most likely a good idea in the circumstances. There is also the the National Security and Intelligence Review Agency, NSIRA, that plays a role and is also an independent oversight body.

You have at least three institutions in total providing a measure of trust: the courts, the OPC and NSIRA, which are independent from the executive branch.

Your study is about, given the intrusiveness of this technology, whether the safeguards should be improved. It may well be that the answer is yes.

Mr. Ryan Williams: In that role, the RCMP mentioned yesterday that sometimes this technology is used in active investigations.

Can you explain, having been in the role for so long, how a PIA protects technology that perhaps may be used in allowing the government to use it in such a way where you're doing an investigation or a PIA? How are you protecting that technology being used in active investigations? What steps can you recommend be implemented to do so?

● (1140)

Mr. Daniel Therrien: I think that speaks to the fact that there are many players, and each should play its role without duplicating the role of others. The courts have an important role, but the courts are bound by the terms of part VI of the Criminal Code. The Office of the Privacy Commissioner looks at privacy more broadly under its statute, and it can therefore provide additional assurance to the public that privacy writ larger than the Criminal Code will be respected when these tools are used.

Each of these mechanisms has a level of confidence. To put it differently, the fact that part VI exists does not mean that that OPC does not have a role. It does have a role.

The Chair: Thank you.

Now, for up to five minutes, we have Mr. Hardie.

Mr. Ken Hardie (Fleetwood—Port Kells, Lib.): Thank you very much, Mr. Chair.

Mr. Therrien, this is a fascinating topic. I'm happy to sit in for my colleague Greg Fergus today.

Judicial authorization is required. Is it required for more than just the incidents and the use of technology that we're talking about here? Are there other areas of investigation where judicial authorization is also required?

Mr. Daniel Therrien: Generally, under the Criminal Code, if there's an invasion of privacy through the use of investigative techniques—wiretaps would be a traditional method—judicial authorization is also required. Search activities, obviously, which do affect privacy, require judicial authorization. There are a number of manifestations of invasions of privacy that require judicial authorization.

Mr. Ken Hardie: Are you aware when judicial authorizations are provided? Are you given a heads-up that there is activity going on?

Mr. Daniel Therrien: No, on the basis that courts provide independent oversight, and it's a mechanism that works on its own.

Mr. Ken Hardie: Are you confident the privacy impacts that the courts assess when they're providing this authorization are reasonably well in line with the terms and conditions that you oversee?

Mr. Daniel Therrien: I'm confident that the courts apply the law correctly. If there's an error, there are appellate mechanisms to ensure that the law is applied correctly. I think it goes back to part VI of the Criminal Code that sets the standards for the courts having a certain definition of privacy, and the Privacy Act has a broader definition of privacy. The fact that I have confidence that the courts do their job correctly does not mean that the OPC applying a slightly different definition does not have a role as well.

Mr. Ken Hardie: Notwithstanding the confidence you may have in the courts is there an auditing mechanism that you would be involved in to go back over the authorizations that the courts have provided to see if, in fact, everything is perfectly synchronized?

Mr. Daniel Therrien: My answer to that would be that the role of the OPC might be to look into how the authorization process worked in individual cases, not with a view to be revisiting what the courts had done—that would be inappropriate—but with a view to determining whether the legislation is sufficient to protect the privacy of Canadians.

Mr. Ken Hardie: We've been focused on the activities of the RCMP. Do similar provisions exist for CSIS?

Mr. Daniel Therrien: There are different provisions for CSIS and for the CSE, the Communications Security Establishment, for the interception of communications. Do these institutions use ODIT-like technology? I don't know, it's quite possible, but there are certainly laws governing the use of technology for the interception of communications by CSIS and the CSE.

● (1145)

Mr. Ken Hardie: In the case of Jeffrey Delisle, the navy officer who was ultimately convicted of espionage, we received a lot of information through the FBI. I don't know that we could be confident that the FBI would follow the same rules with the use of technology that we would. Perhaps they would, but would there be any challenges, especially in the courts, with the admissibility of information that was collected and passed on by another security agency outside of Canada?

Mr. Daniel Therrien: That's a difficult question to answer in the abstract.

I believe Mr. Delisle was convicted, and therefore, the court in question certainly had to be confident of the admissibility of the evidence against the accused. Again, there's important judicial oversight. I will leave it at that.

Mr. Ken Hardie: If you were in possession of more information about what's going on when judicial authorizations are provided and what's actually taking place, why it was provided, etc., especially during an ongoing investigation, would you be compromised in terms of your obligations to Parliament to report and obviously be accountable for the application of the law?

The Chair: I'm really sorry; I was slow there on the hook.

Mr. Hardie, you began that question when your time was already up.

Mr. Therrien, I don't know if you have a brief answer, or again, we'll have to come back to it.

Mr. Daniel Therrien: I don't think it is the role of the OPC to second-guess the courts on individual cases, particularly on an active investigation. Again, the type of review that the OPC should be doing would be at the programmatic level, not at the individual case level, and certainly not while an investigation is occurring.

The Chair: Thank you.

Now, for two and a half minutes, we have Mr. Villemure.

[*Translation*]

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

I'm going to take the two and a half minutes allotted to me to ask two questions and try to form an overview of the subject.

Yesterday, an RCMP officer raised a question that we didn't have time to consider fully. It concerned potential surveillance of Canadian citizens by foreign powers and businesses. As Privacy Commissioner at the time, were you aware of those practices?

Mr. Daniel Therrien: I didn't have any evidence, but let's say I had my doubts.

Mr. René Villemure: You had a reasonable doubt.

Is that correct?

Mr. Daniel Therrien: Yes, I had a reasonable doubt.

Mr. René Villemure: Do we have a provision that would prevent a foreign power from monitoring Canadians?

Mr. Daniel Therrien: That's a matter of national security and measures that national security agencies take to prevent violations of Canadian law. It's an issue in that area.

Mr. René Villemure: These technologies were described as intrusive. According to one RCMP representative, there have always been privacy intrusions, but the tools have changed.

Isn't too much information being gathered?

Is that information preserved in a secure manner to ensure that data leaks such as the one at Desjardins don't occur? They involve a lot of information.

Mr. Daniel Therrien: Yes, methods for gathering information and intercepting communications have always existed, but this tool takes intrusive information-gathering to a new level.

What the RCMP says may be justifiable, but I don't agree that the use of this tool shouldn't have been subject to a privacy impact assessment given its extremely intrusive nature. The commissioner's office should have been consulted.

Mr. René Villemure: Thank you.

Mr. Daniel Therrien: Did I answer your question?

Mr. René Villemure: Yes, very well.

Yesterday, we didn't hear about less intrusive tools that could do the same job.

Do you have an opinion on that?

Mr. Daniel Therrien: Once again, that involves the role of the Office of the Privacy Commissioner and the courts. According to one of the criteria set forth in part VI of the Criminal Code, the court must be satisfied that no other means exist to achieve the desired result, which is to gather evidence. The commissioner's office may have a role to play regarding programs, but we already have provisions requiring the courts to consider the matter.

Mr. René Villemure: May I have five more seconds, Mr. Chair?

[*English*]

The Chair: No, you're over. Sorry.

● (1150)

[*Translation*]

Mr. René Villemure: Thank you very much.

[*English*]

The Chair: Now we have Mr. Green for two and a half minutes.

Mr. Matthew Green: Thank you.

Given the commentary on the intrusive nature of this, the expansive nature of this type of technology, do you believe that the use of this technology by law enforcement has the potential to violate others' charter rights and freedoms?

Mr. Daniel Therrien: Yes.

Mr. Matthew Green: Are you familiar with some of the work that has happened in Europe on the investigation that happened around Pegasus and NSO? In particular, in 2018, the Council of Europe adopted a protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Basically, the principles underpin the rights guaranteed by the European Convention on Human Rights and establish new principles, including the concept of privacy by design.

Do you believe that the principle of privacy by design should be a standard practice for any new technology that law enforcement agencies would like to use?

Mr. Daniel Therrien: Absolutely.

Mr. Matthew Green: Could you take a bit of time to define for people who might not know what privacy by design looks like and how it might be applied in this regard?

Mr. Daniel Therrien: I've referred frequently during the last few minutes to court oversight. Court oversight, *ex post facto* oversight, whether by the courts or the OPC, is necessary, but it is far preferable for privacy to be baked into processes that lead to the use of particularly intrusive technology. The benefit of privacy by design or privacy impact assessment is essentially to ensure that the population can be assured that it's not only after the fact that a violation will be found, but that violations will be reduced greatly in number because the right processes have been put in place.

Mr. Matthew Green: Would you agree that would also include the principles of transparency and accountability?

Mr. Daniel Therrien: Yes.

Mr. Matthew Green: We do know, in fact, that the RCMP in the past, particularly when it used stingray, the IMSI technology for mass surveillance, wasn't actually forthcoming about its use. In fact, it led to particular cases being thrown out of court. I just want to take this moment to underscore those principles—we talked about preamble versus legal frameworks—of transparency, accountability and privacy by design ought to be baked into all processes of law enforcement.

Mr. Daniel Therrien: Yes, and I would—

The Chair: Thank you.

I don't think that was a question. In any event, there would be no time for an answer.

Mr. Matthew Green: If he's going to agree to it, then it goes on the record and becomes part of the committee's Hansard.

The Chair: Okay, I'll allow him to agree.

Mr. Daniel Therrien: I agree, but again, I encourage you to give not very prescriptive definitions to these concepts but some general definition.

The Chair: Thanks.

We will go now to Mr. Kurek, and then we will finish with this witness with five minutes from Ms. Khalid.

Go ahead, Mr. Kurek.

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

Mr. Therrien, it's good to have you back before the ethics committee.

I'll try to get into a bit more detail in what has been an interesting discussion. In particular, we see the responses that the minister gave yesterday. He refused to disclose whether or not.... In a roundabout way, he did acknowledge that when other agencies do, in fact, use ODITs.... In a sense, he indirectly admitted that this type of technology is used by other agencies under the Minister of Public Safety's purview.

If you had a chance to listen to his testimony yesterday, are you concerned about the lack of forthcomingness that the minister displayed before this committee yesterday?

Mr. Daniel Therrien: I would again encourage you to clarify the law. If you want more transparency, make it a legal requirement and define the concept. Speaking about the RCMP for instance, the RCMP's premise, and perhaps that was behind the minister's answer yesterday, is to try to be transparent but to protect its methods of operation so that criminals do not know how they function, because of course investigations would be impeded. This question of protecting methods of operation is always in the minds of police and government officials answering questions like this.

I heard yesterday something that looked like a standard to me, which you might wish to consider. It would be that the government and the police would have an obligation of transparency, subject only to what is necessary to protect police methods and the integrity of investigations. In other words, the standard would be transparency.

The exception would be limited only to what is necessary. Perhaps if that was clearer—not perhaps. It is clear to me because I've had many occasions—and I'm not speaking about the minister; I'm talking about conversations over the years with law enforcement and national security, and it's not their starting point to say things that might impede their investigations. Sometimes they're overly cautious in assessing the balance between transparency and the protection of methods.

If the law was clearer that transparency is the rule and only when necessary to protect police methods is it acceptable to not be transparent, there might be progress.

● (1155)

Mr. Damien Kurek: On the question I asked your successor yesterday, I think it would be valuable to have your response as well.

When you were commissioner, did the Office of the Privacy Commissioner take steps to ensure that, if questions about operational integrity or the status of an investigation were to be part of the conversation around whether or not the privacy of Canadians would be protected in terms of consultations with the Office of the Privacy Commissioner, those things would be protected?

Mr. Daniel Therrien: The OPC has employees who are security cleared. This was made clear to national security and law enforcement, who understand that. Yes, these steps were taken.

Mr. Damien Kurek: Thank you.

Then—

The Chair: Mr. Kurek, I'm sorry, but your time is up.

Mr. Damien Kurek: Okay.

The Chair: Now we have Ms. Khalid for the next five minutes.

Ms. Iqra Khalid (Mississauga—Erin Mills, Lib.): Thank you very much, Chair, and through you, thank you, Monsieur Therrien, for your presence here today.

I'll continue along the same line of questioning that my colleague Mr. Kurek started with. This is with respect to the role of ministers in providing that oversight and how much of a say they have.

Yesterday we heard some testimony that the use of the technology we're talking about dates back to 2012. This means that either Vic Toews or Steven Blaney was the minister at the time. Do you think the RCMP consulted with either Minister Toews or Minister Blaney before deploying that technology?

Mr. Daniel Therrien: Before deploying ODITs?

Ms. Iqra Khalid: Yes.

Mr. Daniel Therrien: I don't know. I heard Minister Mendicino say that this would be an operational issue as opposed to a policy or legislative issue. It may be that the RCMP decided to deploy the tool as an operational matter without informing or seeking authorization from the minister of the day. I don't know.

Ms. Iqra Khalid: Thank you.

As the previous Privacy Commissioner of Canada, did the RCMP ever consult you before deploying this technology at the request of ministers like Minister Toews or Minister Blaney? Did either minister request or approve of a PIA, a privacy impact assessment? Did you ever receive such a PIA during that time?

Mr. Daniel Therrien: I did not know, the OPC did not know, that the police were using this tool, so no, we were never consulted on this in the past.

Ms. Iqra Khalid: Do you know if the RCMP has used any of the software developed by the Awz group, which former prime minister Stephen Harper is deeply involved with, such as Corsight, their facial recognition software, or viisights, their behavioural recognition software?

● (1200)

Mr. Daniel Therrien: I have no knowledge about this.

Ms. Iqra Khalid: We are wandering into fresh territory here for conspiracy theorists at home to listen to this and come away with the idea that the RCMP is doing mass surveillance. Do you think that's true? Is the RCMP conducting mass surveillance on Canadians?

Mr. Daniel Therrien: I don't think so. They said they use ODITs only with judicial authorization. I accept that. With regard to the course of our investigation on facial recognition, are they using mass surveillance? Probably not, but they are certainly using intrusive tools without necessarily clear legal safeguards and independent oversight.

Mass surveillance can take a number of forms, apparently not through ODITs—probably not at all, but I don't know.

Ms. Iqra Khalid: We've had conversations from other members speculating on the role of preambles and making them into legislation. How important is it, do you think, to preserve the discretion of RCMP officers as they're conducting the work of security and protection of Canadians? Where's that balance of ensuring that privacy is protected with that oversight, which is very important?

Do you believe that creating rigid rules and regulations around that privacy, which, in these 32 cases that we're talking about, only intruded in the privacy of those who were being investigated for some very, very serious offences like terrorism, like murder, like trafficking...? Do you think that discretion should be allowed to the courts, to RCMP officers, in the role that they play? Where is that balance?

Mr. Daniel Therrien: You started your question with a reference to preambles and then moved on to whether there should be prescriptive rules. My answer is that of course government officials, including the police, ultimately have a role to play under the law. The law should not be overly prescriptive, but at the same time, I think it is your role as parliamentarians to provide good guidance—maybe not overly prescriptive guidance, but good and substantive guidance—to government officials on how to exercise their responsibilities.

To have in the preamble to the Privacy Act the idea that privacy is a fundamental right I do not think is prescriptive, and I think would be good, sound general guidance to give to the RCMP.

The Chair: Thank you.

Ms. Iqra Khalid: Chair, if I may, I'm just wondering if it would be possible to have Monsieur Therrien stay a little bit longer for the second hour as well. I know that my colleagues have questions as well.

The Chair: Well, I had planned to split this into two panels with the two individuals, but I don't....

I think it would be up to Mr. Therrien if he wishes to remain.

Mr. Daniel Therrien: I'm happy to stay.

The Chair: This wasn't how I had planned to do it, but okay.

Ms. Iqra Khalid: Thank you very, very much. I appreciate that.

The Chair: I have a point of order from Mr. Green.

Mr. Matthew Green: It's just to make sure that we're clear that the extension of Mr. Therrien still allows for resetting the clock on the rotation. We're not melding these together. We get two separate sessions.

The Chair: Yes. I had planned to ensure that these two separate witnesses from our motion would each constitute their own panel for that purpose. Mr. Therrien is welcome to stay, and members may ask him questions, but I understand that Ms. Polsky is already on and is audio tested. We'll go straight into it without....

Monsieur Villemure has a point of order.

[*Translation*]

Mr. René Villemure: Mr. Chair, I just want to ensure that we hear enough from Ms. Polsky because I'm afraid the party opposite is trying to avoid hearing her. I'd like to make sure we can ask her all the questions we want. I love listening to Mr. Therrien, but all the same…

[*English*]

The Chair: All members will be able to ask whomever they wish.

Mr. René Villemure: That's fine.

The Chair: As I said, we will reset the rounds.

With that, I'd like to begin, because I'd like to end this as close to one o'clock as we can to then deal with a couple of items that need to be disposed of.

I welcome Ms. Polsky to our committee and invite her to begin with opening remarks of up to five minutes.

● (1205)

Ms. Sharon Polsky (President, Privacy and Access Council of Canada): Thank you, Mr. Chair.

Good morning from here in Calgary.

To you and members of the committee, thank you for inviting me to appear before you today.

In 1964, Ronald Reagan said, “Freedom is never more than one generation away from extinction.”

In 1992, our Supreme Court said, “The very efficacy of electronic surveillance is such that it has the potential, if left unregulated, to annihilate any expectation that our communications will remain private.” The Supreme Court also said that we have a right to know when the state intrudes on our privacy.

The need for this study tells us that the court has been ignored.

As we saw with Clearview AI, police sometimes sampled data-oriented policing tools with no procurement paper trail, tools they say are needed for public safety to guard against perceived threats or, as Bill C-27 allows, to provide for societal benefits. Put another way, technology itself is morally neutral. How its use is justified makes all the difference, which is why it is so very important that this study is not hidden behind closed doors shielded from full public view.

We know that the Stasi secretly spied on its citizenry, but we don't expect democratic governments to spy on theirs, yet it's now happening in Canada and around the world with journalists, executives, social activists and elected representatives whose views differ from the ruling party being spied on.

Until recently, though, Dudley Do-Right and Sergeant Preston were what people thought of when they thought of the RCMP, defenders of justice and fair play in their relentless pursuit of lawbreakers, respecting the intent in the letter of the law, the charter and Canadian's privacy, not using an unreported surveillance program to spy on Canadians' social media accounts.

Granted, spyware can help police do their work. More often, though, it's downloaded by the hundreds of thousands and used by human traffickers to control sex slaves and, in domestic conflicts, to terrorize partners.

It's also part of a lucrative new sector that's made our privacy, our freedom and our democracy only a crisis or an election away from extinction. How can any MP or bureaucrat be certain that cabinet confidences, military strategies, election plans or anything can be discussed privately when there's a very real chance that a hidden app is letting someone somewhere in the world listen, watch and record your every text, email and photo, siphon your contacts and your passwords and silently turn on the microphone and camera to watch and listen to you and your surroundings undetected?

As for the question of whether there are any social benefits in spyware, the answer is a perverse but resounding yes. It's the Ford Pinto of technology, a danger hidden to the public in general and to certain people in particular with lots of socially beneficial spinoff jobs, commerce and taxes.

The global cybercrime industry generates more than $1.5 trillion U.S. annually. The global cybersecurity industry is at $1.7 trillion and in Canada, it accounts for $3.5 billion U.S. right now.

Pegasus is just the latest spyware to make the headlines. It reminds us that spyware is a non-partisan, equal opportunity endeavour and that the post-911 tools to combat terrorism have made us all fair game to be targeted and our words used against us. Maybe they already have been.

Disrupting the mercenary surveillance industry will require multi-partisan political will, a coordinated domestic and international effort and a shift in approach to prevent the damage from being done in the first place by regulating the exploitation of privacy. Put the onus where it belongs.

Spyware developers, producers, distributors, investors and the inherently faulty technology make the risk greater than the reward, because regulating Internet content won't stop spyware or child predators, and laws banning hacking-for-hire companies and occasionally catching a criminal haven't made a dent.

Using spyware needs to be made unlawful except in specific exceptional situations and for the shortest possible duration necessary to accomplish a specific investigatory goal with its use approved in advance by a genuinely independent, knowledgeable, apolitical third party so that Canadians can regain trust in government and the public sector and have reason to think of Mounties as Dudley Do-Right, not Snidely Whiplash.

● (1210)

The Chair: Thank you for your opening statement.

We go now to Mr. Bezan for up to six minutes.

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

I want to thank Ms. Polsky for joining us today.

How shocked were you, as the president of the Privacy and Access Council of Canada, to learn yesterday under testimony that the RCMP have been deploying on-device investigative tools since before 2012?

Ms. Sharon Polsky: Unfortunately, not at all.

Mr. James Bezan: As you know, this mobile hacking system that's been used on our devices has been banned—Pegasus in particular—from the United States. Are you advocating for this type of technology to be banned or to be used under more stringent guidelines by policing agencies and other organizations?

Ms. Sharon Polsky: I think it's a broader problem than that, because it's not just a matter of banning the police use of a tool that can be used for legitimate purposes, whether by police or other law enforcement agencies. The problem is that these tools, however technically advanced they might be, each one of them, they're available commercially to anybody who has an Internet connection and wants to download them. That is what is the problem, because otherwise, we're all just working after the fact to try to catch whoever is using it.

Our Criminal Code, as far as I'm aware, does not speak to somebody putting spyware on my phone or yours—a spouse, an intimate partner, a stranger. If they take the intimate photos and distribute them without my consent, that's addressed in the Criminal Code, but not spyware itself. Nobody is talking about preventing the spyware from being used in the first place. Nobody is talking about how the spyware is able to take advantage of the shortcomings, the deficiencies in so many software programs.

Google just introduced 27 fixes, including critical fixes, last week in one day. They and others keep introducing fixes for faulty software. Require that software be tested properly to minimize the opportunity for spyware to be able to take advantage right now of the built-in deficiencies.

Mr. James Bezan: Knowing that some of this is available commercially, which I learned just in the last 24 hours.... We've talked about Pegasus, but now there's also Paragon, Candiru, Cognyte software. There's a possibility this has been onboarded onto drones.

Which examples or which software platforms are you aware of that have been used here in Canada?

Ms. Sharon Polsky: I don't know specifically. I have spoken with colleagues who have been researching this area and I've been assured there are several, but it's not spoken about. Obfuscation is a wonderful thing. If you describe a tool as a digital investigative tool, it doesn't say that it's spyware. It gives it the air of legitimacy. I don't know in particular which is being used and which is not.

Mr. James Bezan: Do you believe that Minister Mendicino yesterday was obfuscating? Do you think that after his testimony he restored trust in our institutions on whether or not they are surveilling Canadians?

Ms. Sharon Polsky: I found his responses interesting, particularly when he repeatedly assured us that these software tools are only used within the limits of the law, although, I believe it was he, or perhaps it was someone else, who said that there are provisions in national security law that allow for the exigent use of these without judicial authorization. Even that is within the limits of the law.

Mr. James Bezan: Yesterday there was the admission that the RCMP had been using ODITs since 2012 and before, but he skirted around the issue of whether or not other government agencies are using it.

Do you believe that Canadians have the right to know whether CSIS, CSE, CBSA, the Department of National Defence are using these tools as well?

Ms. Sharon Polsky: I think Canadians do have a right to know. It is possible to reveal the use of these tools without compromising police investigations.

● (1215)

Mr. James Bezan: How dangerous is it to our civil liberties and our ability to appropriately legislate the use of these tools when we have a government that has not admitted the basic facts of who's doing what with ODIT?

Ms. Sharon Polsky: I do recall that our Prime Minister several years ago said Canadians deserve—I'm paraphrasing—the most transparent, accountable government. I agree that we do, but as a taxpayer, as a Canadian citizen, I'm skeptical whether that has come to pass. As a practitioner in access and privacy for many, many years and knowing many people in the industry, including in our nation's capital, it seems that the way the access laws were written is being used to create more of a shield than a view of what's going on.

The Chair: You have 10 seconds.

Mr. James Bezan: I want to thank our witnesses for being with us today.

The Chair: Thank you, Mr. Bezan.

Ms. Hepfner, you have the floor.

Ms. Lisa Hepfner: Thank you, Chair.

I would like to return to Mr. Therrien and some of the conversations that we were having in the previous hour.

There have been a lot of suggestions that judicial oversight isn't enough. I think what I heard from you is that it's pretty good protection and that it's not the only protection that we have to ensure that the RCMP fulfill their mandate to the letter of the law. For example, if they were to collect information through the use of this technology and take it to the court to use in prosecuting their suspects, and the court found that they didn't use it properly, then the evidence is no good and it's worthless to them, so it's no good for the RCMP to be using this technology outside the letter of the law.

I'm wondering if you agree with that and if you could expand on that a little bit.

Mr. Daniel Therrien: I think it's a fair characterization of what I said. The privacy safeguards in part VI of the Criminal Code are good. They may well be perfectible, particularly given the highly invasive nature of ODITs.

Ms. Lisa Hepfner: Please expand on that. What do you mean?

Mr. Daniel Therrien: Yes, the protections of the Criminal Code are good. Are they ideal? Are they perfect? Are they perfectible? I leave that to you. I think that certainly improvements are possible, but they are good. We have a good starting point.

Ms. Lisa Hepfner: We also heard, as one of my colleagues brought up yesterday, that we may be more at risk in terms of MPs and our cellphones from outside actors and people outside the country who maybe aren't concerned with following the Criminal Code. Can you expand on your thoughts on that as well and the level of risk in this country from outside of Canada?

Mr. Daniel Therrien: Canadian law governs Canadian institutions, including the RCMP, and by and large, we have good rules. As we know, there are a number of countries around the world that are not democratic and do not care much for the rule of law, and it is entirely possible, likely—the RCMP seem to suggest it's a fact—that other states do intercept the communications of foreign nationals, including Canadians, for their own purposes. According to the RCMP, it's a fact.

Ms. Lisa Hepfner: How does Canada compare to other countries when it comes to valuing the right to privacy of its citizens?

Mr. Daniel Therrien: Clearly, Canada is a country under the charter, the rule of law, and overall has good standing in defending human rights. At the same time, it was mentioned a few minutes ago that the public sector privacy law is 40 years old. The law was adopted when documents held by the government were held in writing in filing cabinets and the information could not be obtained or disclosed as easily as it is in 2022.

Overall, obviously we are a country that respects the rule of law, but our laws, particularly privacy laws, are in dire need of improvements from a privacy perspective.

● (1220)

Ms. Lisa Hepfner: In the minute and a half or so that I have left, maybe you could go over some of your ideas, which I'm sure you've already brought up today, for improving our privacy laws to make sure that we are at the highest standard.

Mr. Daniel Therrien: Canada's laws, for both the public and the private sectors, should recognize privacy as a fundamental human right. That's the starting point. We should ensure that the Office of the Privacy Commissioner, for both the public and the private sectors, has the authority to not just make recommendations, but make orders for the private sector and the public sector when it sees violations of the law. There should also be financial sanctions, certainly in the private sector, to ensure that these laws are respected.

I would say, because I think it's relevant to this particular study and it was referenced a minute ago regarding the use of these intrusive technologies in the private sector, that in 2022, information is shared between the private and public sectors extensively, and it is important that at the very least, public sector and private sector laws are compatible and interoperable. Ideally, they should be adopted in one statute, because data does not know frontiers between the public sector and the private sector. Again, at the very least, the rules should be similar and interoperable as between the public and private sectors.

Ms. Lisa Hepfner: That's very helpful. Thank you.

The Chair: Thank you.

[*Translation*]

Go ahead for six minutes, Mr. Villemure.

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

Good afternoon, Ms. Polsky, and welcome to the committee. We are very pleased to see you today.

We've been discussing privacy and trust from the start. We want to establish and maintain trust.

Many fellow citizens in my riding tell me they have nothing to hide and therefore wonder why we have to address these issues. I'm not sure people understand the intrusive nature of spyware, for example.

Would you be able to explain to us what our fellow citizens are dealing with so we can explain it to them?

[*English*]

Ms. Sharon Polsky: Well, they're saying, “I don't have anything to hide”, but people have said that to me and I've said, “Show me your bank statement” and they get weirded out by it. People do have things to hide, but it's more a matter of the idea that when I wish to share a particular bit of information about me, I should have a choice.

For those who want to display their life online, the minutiae of their lives, that's their choice, but, to paraphrase Senator Simons, governments aren't always benevolent. I look to Hungary and Poland, but to Hungary in particular, which has changed in recent years to become rather authoritarian. Its data protection authority, which you would expect to have a role similar to that of our Privacy Commissioner, has ruled that the use of Pegasus against the country's journalists does not violate the law because there is a national security component.

Things that are okay today can be changed on a whim these days, used against you and taken out of context. That's nothing new; that's gone on from time immemorial, but we need to have the choice. Having our information or information about us gathered, taken, assembled, assessed and analyzed by someone we don't know, we've never met and we've never given permission to—what are they going to do with it?—means we're looking at McCarthy hearings again. It's frightening.

I've been around a long time and there's not a lot that scares me. What's going on now is frightening, and that's what people need to realize. It's not just benevolence.

● (1225)

[*Translation*]

Mr. René Villemure: Do we need to have a public debate on privacy or awareness programs so people are in a better position to understand what they're dealing with?

[*English*]

Ms. Sharon Polsky: Oh, that would be wonderful. Desktop computers have been around for almost a half a century, and as far as I'm aware, there really isn't any substantive education yet, whether for schoolchildren in the youngest grades or even people in university. They're taught to code perhaps, but not everybody needs to code, and knowing how to code doesn't mean you understand privacy—what privacy is, how it can be undermined and how to protect yourself from clicking on the wrong thing and endangering your device, your enterprise and perhaps, in your case, the nation because of national security.

I have spoken with a variety of members of the bench from across the country over the years, and one after the other has said, “I don't know what this privacy stuff is. I'm at this conference to learn it, even though I'm adjudicating matters that are sensitive as to privacy.” There has not been enough education, and there needs to be a dedicated mandatory education component embedded as a pan-Canadian strategy, if you will, so that the provinces and territories can have the encouragement to embed this as a mandatory part of the curriculum, starting at the youngest grades.

[*Translation*]

Mr. René Villemure: For the moment, shouldn't we impose a moratorium on the use of these technologies until we can understand them better and, in our case, can explain them and legislate more clearly?

[*English*]

Ms. Sharon Polsky: Well, it would be lovely, but we've seen moratoria declared on facial recognition in the past few years by various cities, states and countries, and now they are sliding back to saying that maybe it would be a better thing if they had it. That's a temporary measure. I think it's more important to get to the source of the problem, which is the faulty software that provides the opportunity for spyware, ransomware and other malware to be effective.

[*Translation*]

Mr. René Villemure: Thank you very much.

[*English*]

The Chair: You have another minute.

[*Translation*]

Mr. René Villemure: Mr. Therrien, I'd briefly like to go back to a point you raised. The right to privacy is addressed in many bills and has been subject to numerous revisions in statutes concerning the private and public sectors.

Wouldn't it be a good idea to create a single statute? I realize that would be complicated, but it might help correct existing deficiencies in the statutes in question.

Mr. Daniel Therrien: That's the case in certain countries. Since data travels, as it were, between the private and public sectors, that would be a good idea.

However, I would add that we waited 40 years for amendments to the Privacy Act for the public sector and 20 years for amendments to the act concerning the private sector. The risk involved in combining it all in a single act in Canada today is that it might delay passage of the act respecting the private sector, which is currently before Parliament.

In principle, the public and private sectors should be regulated in a similar manner. The contexts are somewhat different, but the statutes should be based on similar, if not identical, principles.

Mr. René Villemure: Thank you very much.

[*English*]

The Chair: Thank you.

Now we'll have Mr. Green for up to six minutes.

Mr. Matthew Green: Thank you very much.

Mr. Therrien, I'm sure you would note that the President of the Treasury Board is responsible for establishing policies and prescribing forms regarding the operation of the Privacy Act in the public sector. We know that they've had this mandate for quite some time.

Given your time as Privacy Commissioner, could you comment on the rate at which ministries and agencies under the Privacy Act have proactively presented policies and measures for outcomes and accountability within their departmental plans in reporting back to public accounts or to your office? Did you feel they kept pace with technology as it is today?

Mr. Daniel Therrien: That's an excellent question.

I would say that during my term, Treasury Board, as a matter of priority, because of limited resources probably, spent more time on access to information questions than privacy questions. They were not absent from the privacy landscape, but they certainly gave priority to access to information. There was an access to information bill presented, etc.

The long and short of it is that there was not an absence of activity, but there was not a whole lot of activity.

● (1230)

Mr. Matthew Green: Is it safe to say that even though in spirit the policy of the Treasury Board was directing all agencies to enact enhanced protections under the Privacy Act, it didn't necessarily result in proactive new policies that are in keeping with the pace of technology today?

Mr. Daniel Therrien: Yes, although I will say that in the recent year or so, there have been interesting developments—a policy on artificial intelligence, for instance—but over my term, there was not a whole lot of activity. There has been more progress recently.

Mr. Matthew Green: In the time of your term, how much of that activity in proactive improvement, in self-reflection and auditing, came from law enforcement and public security agencies, with specificity around the RCMP? Was the RCMP leading the way in improving their processes around privacy?

Mr. Daniel Therrien: No. If we look at facial recognition and the creation of what they call NTOP, it was at our request. It was not proactive on their part.

Mr. Matthew Green: Sure. Is it also safe to say that in some of your dealings—I hope we can be candid here—they maybe weren't always forthcoming with the information as necessary for you to be able to fulfill the duties of your work in a timely manner?

Mr. Daniel Therrien: I think they functioned within the law as it is.

Mr. Matthew Green: That is an important distinction, because what's before us today isn't necessarily a positioning of the RCMP as being rogue or going outside the confines of the law, but it's the gaps, I would argue. In fact, Deputy Commissioner Larkin in his testimony suggested there were gaps in legislation.

Would you also then agree that even though what is currently legal, and I think we've established is quite outdated, it might not necessarily be ethical, given the way in which technology has outpaced legislation?

Mr. Daniel Therrien: Whether it's ethical or not, there are certainly improvements that are possible, given the intrusiveness of the technology, beyond part VI of the Criminal Code. Yes.

Mr. Matthew Green: I think there would be a long debate on the ethics of it, but I would put to the committee that if we have technology that goes beyond the spirit of existing legislation, and is known to be such, then in some instances, whether it's the stingray or operation Wide Awake, which was the social media surveillance, or others, if they're not proactively disclosing these things, then it doesn't give legislators the opportunity to keep up with it. I think that's the spirit of what's before us here today.

I referenced the European Convention on Human Rights, which established transparency, accountability, privacy by design and data protection impact assessments . That's a relatively modern piece of legislation. In your mind, how does Canada compare with that?

Mr. Daniel Therrien: We by and large have policies, not always respected, that have a similar spirit, but they're not legal requirements. I think it would be extremely helpful to change these policy rules into laws so that the likelihood that they would actually be implemented would increase significantly.

Mr. Matthew Green: I would agree. In my position, having been on public services and procurement and public accounts and now this committee, we have a government that is really great at writing good policy. They actually write some decent policy. The challenge is that we never have the outcomes. We never have the measurables. We never have the deliverables when it comes to taking something like the directives of the Treasury Board president and watching them actually be implemented in government.

From that perspective, what I'm hearing today, and we can get into distinctions between whether or not it's prescriptive or non-prescriptive or whether or not it's preamble, I'm a firm believer that if we don't direct law enforcement to improve, to increase their transparency, and to provide clear measures of accountability and privacy by design, it won't happen.

Would you agree with that, that if we don't provide those guidelines, it just won't happen?

Mr. Daniel Therrien: Yes. Further, I think it is possible to have these requirements at a sufficient level of generality, but still meaningful, without being overly prescriptive and preventing officials, whether by the police or others, from exercising judgment. But—

● (1235)

The Chair: Thank you.

Mr. Matthew Green: Thank you.

The Chair: We'll go now to Mr. Williams for up to five minutes.

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

Ms. Polsky, it's nice to see you again.

After the RCMP was caught having used mobile device identifiers, or IMSI, in 2017, they said they wanted to start a public debate about police powers and privacy. That discussion was clearly never started. Do you agree with that statement?

Ms. Sharon Polsky: I'm not aware that they did engage in that study.

Mr. Ryan Williams: Do you think that the balance between police powers and privacy should be changed? What should it look like?

Ms. Sharon Polsky: I think police need to recognize that they're not always going to be in uniform and that it affects them individually just as easily as it does you and me and anybody else.

Members of law enforcement are like everybody else. They, too, lack the fundamental education about privacy rights and responsibilities and legislation. They are law enforcement, and that's what they do. They see it from that perspective, as they ought to, but they need to be encouraged to see it from other perspectives.

Mr. Ryan Williams: What does Parliament need to do to properly regulate these types of uses of spyware by the RCMP, CSIS and CSE, for example?

Ms. Sharon Polsky: First of all, I think if the spyware is regulated in the hands of RCMP and federal agencies, that doesn't address the municipal and the provincial law enforcement agencies, so it has to be all encompassing.

I think it's a matter of crafting laws—again, without the direct or indirect influence of industry—that put the liability first on the hardware and software companies and their executives who sell products that are full of vulnerabilities that allow spyware, ransomware and malware attacks. Ban federal procurement or use, directly or indirectly, of spyware by legislation, regulation or order in council, with equivalent bans in each province and territory, and work with foreign governments to ban the sale, export, distribution, use of and investment in commercial spyware.

We already have international free trade agreements that have mandatory cross-border information-sharing provisions and all sorts of other provisions. They need to include provisions where signatories agree to criminalize and prosecute the individuals and the organizations that create, test, market, fund and distribute spyware—and the executives and the investors. There have to be penalties because, otherwise, it's like policy: It's on the books, but if someone in another country can use these products against us, their own governments have to be involved in stopping it because that's in that country, of course. It's out of our reach.

Mr. Ryan Williams: To just add to my colleague's sentiment or statement earlier.... What good policy has actually been implemented in other countries that we should be implementing here in Canada?

Ms. Sharon Polsky: One of the most important differences, I think—a distinction—that the GDPR in Europe brought to bear is that when a privacy impact assessment is conducted, when an organization has a data protection officer, which they must, their focus under the GDPR is the risk to the individual whose information is being collected, used, etc. It's not the risk to the organization. In my experience, that is all too often how Canadian organizations look at it.

First of all, if they have a preliminary PIA—because we're busy; we're a large organization—the few people who actually understand it are too busy to do a PIA for everybody, so they ship it back to the department and say, “Here, you do a preliminary PIA, and you tell me if you think we need to do a PIA.” They don't know what they're looking at, so of course it's easy to say, “Nah, it doesn't affect personal information, so we don't need a PIA.” That's where it ends. That's a flawed system.

When they do do a PIA, some of them are just so cursory. It talks about the benefits of a product or a new system or something, but it doesn't talk about the risk to the individual. It's as if their role is to protect the risk of the organization. That has to change.

● (1240)

Mr. Ryan Williams: Mr. Chair, my last question for—

The Chair: You're—

Mr. Ryan Williams: It'll be for a yes or no. That's all it'll be.

The Chair: You have 10 seconds.

Mr. Ryan Williams: This is for both witnesses: Should skipping the PIA be an option at all?

Mr. Daniel Therrien: No.

Ms. Sharon Polsky: No.

Mr. Ryan Williams: Thank you very much.

The Chair: Well done.

Now, we'll go to our next questioner, who will be Mr. Erskine-Smith.

Welcome back to the ethics committee.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Thanks, Pat. It's good to be back. It's good to see you.

It's especially good to see you, Mr. Therrien. I have appreciated your advice and guidance over the years when I did sit on this committee.

I want to start with what I took to be the RCMP's view around “We can't disclose the vendor because of national security.” Yet, from a government procurement basis, it's quite concerning to me, because I see some of this technology—and I know the RCMP has said it doesn't use Pegasus, but Pegasus is an example—has been used to seriously undermine human rights around the world, attacking journalists and other human rights advocates.

As a matter of public interest, shouldn't we know who the vendor is so that we can conduct some level of due diligence around government procurement?

Mr. Daniel Therrien: That there be transparency in the procurement process is certainly a very good idea. It's necessary, actually. On whether the name of a particular vendor should become public, I would go back to the general standard: There should be transparency as a rule, except if methods would become ineffective through transparency.

Mr. Nathaniel Erskine-Smith: I think that's the right standard. It's hard to imagine that having the name of a vendor would undermine national security, despite the protestations we heard yesterday.

Moving to the core issue, we've talked about the nature of the tool and how expansive it is with respect to collecting data, but I want to take a slightly different tack, Mr. Therrien, because what these tools tend to do and what makes them demonstrably different from other tools is they take advantage of and exploit an existing vulnerability in the technology as it is. You have law enforcement that is exploiting a vulnerability, and that vulnerability affects all Canadians fundamentally, because that vulnerability is on all devices.

Isn't there an argument that law enforcement should be identifying that vulnerability and then letting the company know about the vulnerability such that it's fixed on all of our devices?

Mr. Daniel Therrien: It's a daunting question. Yes, if government officials see a vulnerability in a system, they should notify the creator or the vendor of the system of the vulnerability as a principle generally applicable and implemented, yes. That said, encryption is a challenge to law enforcement, so I think I make a distinction between laws dictating the creation of back doors and laws that authorize the police to circumvent encryption through existing vulnerabilities for a certain period, because that may be the only way to actually perform the investigation.

I don't know, frankly, what the best solution is in this regard. I agree with you that there's an obligation to inform the vendor or the creator at some point, but how do the police...? I see what's being done here as less problematic than laws creating back doors, particularly where there's judicial oversight of the system.

Mr. Nathaniel Erskine-Smith: Let's talk about that oversight in the remaining time I have.

I'm comforted that the RCMP has said that they've only used this technology via judicial oversight, but of course, it would have been nice if they were more proactive in their disclosure of the use of this. We now have a pattern, I think, when we look at stingrays, Clearview AI and now this spyware technology, and again, we don't know who the vendor is.

Don't you think the Privacy Commissioner ought to be involved? When I look at the RCMP telling us nine out of 10 requests did not receive internal approval, I don't know what that internal approval framework is, quite frankly. I would think if I were responsible for the RCMP, I would proactively engage with the Privacy Commissioner in establishing that internal framework. Would that make sense to you?

● (1245)

Mr. Daniel Therrien: Yes, absolutely.

Mr. Nathaniel Erskine-Smith: It makes sense to me too.

Mr. Daniel Therrien: That's what we recommended for facial recognition, which led to the NTOP process. Yes, the OPC should be involved in ensuring that these processes are sound and robust.

Mr. Nathaniel Erskine-Smith: Right, because then you have the internal approval framework in consultation with the OPC, and then you have the judicial framework on the back end.

Thanks, Mr. Therrien. I appreciate your public service. Take care.

The Chair: Thank you, Mr. Erskine-Smith.

[*Translation*]

Mr. Villemure, you now have the floor for two and a half minutes.

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

Mr. Therrien, would you say the RCMP has developed a privacy culture?

Mr. Daniel Therrien: The RCMP has a culture of applying the legislation as it stands.

As was said, it's true the RCMP doesn't have particularly extensive privacy expertise. In the past year of my term, I've seen a willingness on the RCMP's part to improve its privacy knowledge, but that's not its initial inclination.

Mr. René Villemure: We're on the right track.

Aren't we?

Mr. Daniel Therrien: Yes.

Mr. René Villemure: In the last round of questions, Ms. Polsky discussed privacy impact assessments, saying they were something we could do but that ultimately might not produce results.

Do you agree with that statement?

Mr. Daniel Therrien: That's partly why I encourage you to make it a legal obligation to conduct PIAs and to include the purpose and content of those assessments in the act.

There's a real risk here. In many cases I've seen, the assessments were a purely mechanical exercise, and that serves no purpose. The aim is to ensure that programs and activities are designed to respect privacy and that privacy is a fundamental right. The idea behind an assessment is to be proactive.

Mr. René Villemure: Thank you very much.

Ms. Polsky, in less than a minute, do you think it's time for a public debate on the subject so citizens can form a clearer understanding of what's at stake?

[*English*]

Ms. Sharon Polsky: Absolutely, and I think Canadians need to be engaged to understand not only what's at stake nationally, but personally. Again, I go back to education, and it's mandatory, because otherwise, they have no option whether personally or in a corporate or government role to take the word of a vendor or someone else, without being able to have critical thought and ask the questions that need to be asked and know if they're getting legitimate answers.

[*Translation*]

Mr. René Villemure: Thank you very much.

[*English*]

The Chair: Thank you.

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

Mr. Matthew Green: Thank you.

I want to go back to the end of my last question. I feel that Mr. Therrien was about to expand on his thoughts around how we can bridge the gap between the policy directives that are instituted under the purview of the President of the Treasury Board with the Privacy Act and all of the boards and agencies, including law enforcement, to begin to build in this culture of the underlying value of privacy as an actual fundamental right.

Mr. Daniel Therrien: The law is crucial here. We have in Canada policies that promote privacy, but sometimes, frankly, they are a little bit hollow. It's a check box exercise. For PIAs and privacy by design to be meaningful, to recognize privacy as a fundamental right, to ensure there is adequate enforcement, including order making and fines, it means that it is no longer possible for either the private or the public sector to speak the good words without actually delivering on privacy protection.

Policies are good, but they need to be backed up by serious legal standards and independent oversight.

Mr. Matthew Green: This is something that we've been kind of circling around at this committee in such a short period of time, responding to the recent use of this particular technology within the RCMP. I think, as you alluded to, it's not confined to that. I think it's safe to say that if the RCMP is using this technology, we're likely to see that the CSE and CSIS levels...although they have different constraints and requirements.

One thing that we didn't touch on was the possibility of the government doing indirectly what it can't do directly. Would you end by commenting on ways in which we might be able to ensure that our government isn't utilizing, even though it might be legal—I would suggest not ethical—unlawful information, unlawfully gained information from our foreign partners within the international security framework with Canadian agencies?

● (1250)

The Chair: Give a very quick answer if you can, because we're out of time.

Mr. Daniel Therrien: I'll answer with regard to the private sector. In the OPC's investigation of facial recognition, we recommend that the law be clarified, that the government, the state, cannot do indirectly through the use of the private sector what it cannot do directly. I think that's a big part of the answer.

Mr. Matthew Green: Thank you.

The Chair: Thank you.

With the final two rounds, we'll have Mr. Kurek for five, followed by Ms. Khalid.

Mr. Damien Kurek: Thank you very much.

Mr. Therrien, are wiretap warrants that are used by law enforcement under the Criminal Code automatically sealed?

Mr. Daniel Therrien: I think they are generally sealed. You're going a little bit beyond my area of expertise here, but they're certainly generally sealed.

Mr. Damien Kurek: Okay. Thank you very much.

Ms. Polsky, there was some very interesting testimony today, so I'm going to ask you a series of questions. One is related to the letter that the commissioner of the RCMP had sent to this committee refusing to disclose some information that this committee had asked for. Is that something that concerns you?

Ms. Sharon Polsky: Very much. My view as a Canadian and as a taxpayer is that government and our law enforcement agencies are there to serve the public, not hide from it. It just doesn't come across as being deserving of trust. Trust has to be earned. To just flatly refuse a parliamentary committee and say no—that was surprising. It makes me think, are they hiding something?

Mr. Damien Kurek: All right. I appreciate that.

Yesterday the minister was not forthcoming when a number of us, including me, asked questions related to the use of national security exemptions. Is it concerning to you that the minister responsible for these agencies would not be forthcoming as to whether or not exemptions were used to circumvent some of the judicial processes laid out in the Criminal Code?

Ms. Sharon Polsky: Well, it certainly is concerning that there's a lack of clarity. It just seemed evasive.

Mr. Damien Kurek: As there are questions about operational integrity and ensuring that the integrity of investigations is upheld, and both the current and the previous commissioner for privacy have outlined how there are safeguards in place, do you find it concerning that it seems as though on this issue and also in previous areas that the RCMP has only responded to privacy concerns after either parliamentary or media outcry related to things like the use of ODITs, Clearview AI in terms of facial recognition, and that sort of thing?

Ms. Sharon Polsky: I think it's a problem that they are not collaborating with the Office of the Privacy Commissioner of Canada in advance but only after they get caught with their hands in the cookie jar. I think they're doing themselves and every law enforcement agency across the country a disservice when they are not forthcoming.

It also puts them on the defensive if they don't come forward and say, “We need to use this type of tool.” It doesn't give away any investigative information. Being general like that doesn't undermine investigations. It doesn't reveal anything sensitive. Help educate the public as to why you need this particular type of tool. Don't wait to be put on the hot seat and then give non-answers, like so many of them did yesterday.

● (1255)

Mr. Damien Kurek: When it comes to specific actions, Ms. Polsky, do you believe it should be outlined in privacy legislation that there should be proactive disclosures as opposed to parliamentary committees or reporters having to chase down the RCMP or other entities of government to try to bring about a public understanding of some of these privacy concerns?

Ms. Sharon Polsky: Yes. Having it in law is necessary. It has to be clear, not open to interpretation by an organization that wants to use the law to its advantage and not for the sake of clarity. But I caution saying, well, we have new legislation, Bill C-27, the artificial intelligence data act, and that will protect it. It doesn't, because any organization that is deputized, if you will, by CSE or CSIS can do what the government can't.

The Chair: Thank you, Ms. Polsky.

Mr. Damien Kurek: Thank you.

The Chair: We'll finish this panel with Ms. Khalid.

Go ahead for the final five minutes.

Ms. Iqra Khalid: Thank you very much, Chair.

Thank you again to the witnesses.

Monsieur Therrien, if you don't mind, I'll continue with you.

Now, we've heard the scope of the spyware and its use and its intrusive nature on not just Canadians but people in general. The European Union has been involved in, for example, putting Pegasus...saying that it is violating rights. Do you think Canadians should be able to sell spyware like Pegasus to anyone at all? For example, I mentioned the Awz group in my previous questioning. Should organizations like those be able to sell this extremely intrusive technology? Should the government be regulating not only the use of that within our country but also the sale of that abroad?

Mr. Daniel Therrien: Yes, there should be laws regulating the sale, import and export of these technologies. Should they be banned completely? We see in this study that there may be rare cases when the public interest would make the use of such technology by the state permissible, but definitely there should be laws around sales, import and export.

By the way, while I can see compelling grounds for the government, the state and the police to use this type of technology exceptionally with judicial authorization, I cannot really see any compelling reason that someone in the private sector should be able to use this technology. Maybe I don't have sufficient imagination, but I cannot see any compelling reason the private sector should be able to use it.

Ms. Iqra Khalid: Thanks very much for that.

I know that members have talked about accountability and the responsibility of a minister, for example, to oversee the work of the RCMP. You have said that operational decisions are not made by ministers and that, in fact, they don't get involved.

Can you perhaps expand on the importance of that division or separation of powers and responsibilities?

Mr. Daniel Therrien: There's certainly jurisprudence by the Supreme Court on the notion of police independence, which defines the limits of political direction over the work of police forces. At the same time, I've suggested that there could be certain legal prescriptions on the police, for instance, through the Privacy Act. The Criminal Code, part VI, which has been referred to frequently, has transparency requirements that are imposed by law on the government and therefore include the police. You may want to have a look at these transparency requirements to see whether they should be improved. They're good, but they are probably perfectible.

Ms. Iqra Khalid: Thank you very much for that.

My last question for you is around the part of the motion that seems to be insinuating that the RCMP is wiretapping or surveilling members of Parliament.

Given your very great experience with the privacy commission and beyond, hypothetically, if members of Parliament were colluding with others in the planning or furtherance of illegal activities in Canada—for example, if they were working with the convoy that occupied Ottawa for a couple weeks—would there be any sort of parliamentary privilege that would interfere with the RCMP's ability to conduct surveillance, including through ODITs, if a proper court order has been obtained?

● (1300)

Mr. Daniel Therrien: No one is above the law, so all Canadians are subject to the law, including criminal law, and can be the subject of investigations.

I think the RCMP stated yesterday that, although that might be a possibility, there are internal mechanisms to ensure that the surveillance of a member of Parliament requires a higher authorization within the RCMP. I have no knowledge that MPs are surveilled in that way, but certainly at the level of principle, no one is beyond the law.

Ms. Iqra Khalid: Thank you very much for that, Mr. Therrien.

The Chair: Thank you. That concludes your time.

First of all, I would like to thank both of our witnesses and excuse them at this time.

We have some time now to address some different pieces of committee business we have, but before we do that, the analysts have asked to have a couple of minutes to brief me, so I am going to suspend. We're going to stay on this call so we remain in public. The meeting is still in force, but we'll be suspended.

● (1300)

_____(Pause)_____

● (1305)

The Chair: The meeting is back in session, so I invite everyone to get back to their seats.

I just have some notes here about this study that may even affect how we proceed with the rest of our day today.

The analysts have informed me of what the production constraints are around completing a report in order to comply with the timelines set out in the motion that we adopted in July, so we will conclude the study today. This will be the last day of testimony for this study.

The quickest that we are likely to get a draft report for the committee's consideration is September 12. We have committed in our motion to table the report the following week.

The week of September 12 is a very difficult week for at least four members of this committee in terms of time availability. Otherwise, it would be an excellent week for us, I'm sure. The point is that I think we are heading toward a very limited possibility of tabling this report within the constraints of the motion. It would be my intention, as the chair, to call the appropriate meetings at my discretion to do our best to table this report in Parliament as soon as possible, given the constraints that both the analysts and the production team will have, translation services as well, and perhaps the limitations of some of our committee members that week.

We may have to have a meeting in that week of the 12th, before Parliament resumes. We'll see.

As far as drafting instructions go, I'm going to ask that members communicate with the analysts through the clerk any particular instructions they might have. That way maybe we can dispense with a meeting dedicated to the production of documents.

I'm not sure how much debate we can have about this. I know that members may want the floor to deal with motions as well.

I see Mr. Green and Ms. Khalid.

Go ahead, Matthew.

● (1310)

Mr. Matthew Green: Thank you.

I think we're getting some really good information here. In fact, in the testimony yesterday, the deputy commissioner of the RCMP volunteered to provide us with the privacy impact assessment, and there was even conversation from the testimony yesterday that they would be willing to be more forthcoming with us in camera.

You'll note in my response to that yesterday that it might be of value to this study to allow for the impact assessment to come back with the potential for an opportunity to revisit the conversation in camera to get the full disclosure and candour of the decisions that were made and how they arrived at those decisions.

I think, absent of that, Mr. Chair, we're going to be missing a significant component of this study, and we'd only then have to come back with some kind of amendment or to reopen it. I think it would be easier, procedurally, if we found a way to adjourn, pause, recess the meeting, whatever the correct procedural language is, until such time that we receive that information and are able to conclude our final thoughts on the drafting of the final report.

The Chair: Thank you.

Ms. Khalid, go ahead.

Ms. Iqra Khalid: Thanks, Mr. Chair. I appreciate it.

I agree with you on the timing piece. I realize the challenges that our analysts will have. I realize also just how much effort they put into making sure that we're well supported in the work that we do.

I'm wondering if it would be feasible that we carry on with this additional meeting and extension of document submissions perhaps by the first week that we get back, the week of September 19. I think it would be very practical, and it would work with all of our schedules, as well as give the analysts enough time to put it all together.

I'd love your thoughts on this, Mr. Chair.

The Chair: The problem with that is—and we're free to change our mind and revisit the decisions we've made—a decision was made by this committee to table the report in Parliament that week. This is why I'm raising this now, because I see the difficulty in meeting what we have committed ourselves to doing, and we certainly wouldn't be able to table the report quickly if we wait until that week even to instruct the analysts to produce the draft or work on the draft.

I have Mr. Bezan and then Monsieur Villemure.

Mr. James Bezan: Mr. Chair, I'll just say that based upon the testimony that we have heard and based upon conversations that Mr. Green had with the RCMP, I think there is value in having some in camera meetings to get more detail. I also think that based upon yesterday's testimony, there's the potential that CSIS and other policing agencies across this country, the CSE and National Defence, may be employing this technology as well, and we may want to hear from them.

Rather than function under a time constraint, and I'll leave it to Monsieur Villemure who brought forward the motion, potentially we should look at extending this study rather than getting in a rush to table the report. I think this is something that we need to delve into in more detail, especially as we start talking about privacy impact statements, updating the Criminal Code to make sure the warrants are sufficient or need to be improved to deal with ODIT.

We also need to be talking to the commercial application of this technology and whether or not, based upon the various vendors that are out there, perhaps we should be hearing from some of them as well, and who is making use of their technology and if it is being downloaded by nefarious actors, whether they be at the state level, or whether they be in the private sector, and how that could potentially impact our privacy as Canadians.

● (1315)

The Chair: Thank you.

That may be where we're heading.

For everyone to be aware, the more meetings we add, the longer this will take to get to the draft.

Mr. James Bezan: That's understood.

The Chair: As long as that's understood, because this is the conflict that is within the existing motion that this study exists under.

Go ahead, René.

[*Translation*]

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

I think we've learned a great deal in these two days of testimony. We have a lot of material to include in an eventual report. However, the goodwill of the RCMP people and their readiness to come back after conducting a privacy impact assessment are essential. We can't conclude our work if we don't see that.

I'm not sure we need to go into all the ramifications that Mr. Bezan mentioned. I think our work would definitely be incomplete if we didn't accept the hand that, for once, the RCMP has extended to us.

[*English*]

The Chair: Thank you.

If I may, I would take from this discussion that there is consensus to have additional meetings, particularly an in camera meeting, and to not rush to prepare the report and table it in the House. If there's consensus around that, then I'll consider that settled and the next meeting will be at the call of the chair, when appropriate.

Mr. Bezan, you have the floor.

Mr. James Bezan: Mr. Chair, with that, I'd like to retable my motion from yesterday. I'll read it into the record:

> 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; and that all documents be circulated to committee members, at the earliest opportunity, once vetted.

Again, to reaffirm to my colleagues, this isn't about a witch hunt. This is trying to understand the mechanics behind and circumstances in which warrants are used for the on-device investigative tools, and that this technology needs to be further looked at. We can do this through the document process, but I don't want to violate people's privacy rights. I don't want to undermine the ongoing investigations that the RCMP are currently involved in, as well as raise any information that is considered a national security risk. We're trying to ensure that the Law Clerk and Parliamentary Counsel has the capability to go in there, redact and vet those documents and give us only the information that we need for this study.

The Chair: Thank you.

Ms. Khalid, you have the floor.

Ms. Iqra Khalid: Thank you very much, Chair.

While I understand the importance of this motion, I would like to move an amendment. The amendment has been emailed to all the P9s of members. I'll read into the record:

> That the motion be amended by adding after the words “original motion” the following: “with the exception of sealed warrants”.

The reason for that, Mr. Chair, is that the seal order is made by a judge. If a judge made a decision to seal a warrant, the RCMP won't have the ability to contradict that or to provide us with that information. Therefore, it just doesn't make sense for us to try to hold the RCMP to account for something that they just are not able to do.

It's a practical motion. Obviously, all of the documents as listed out by Mr. Bezan still apply. I just think that this amendment is a technicality to ensure that we're not asking the RCMP to do something they're not able to do.

● (1320)

The Chair: Thank you.

Is there debate on the amendment?

Mr. Bezan.

Mr. James Bezan: I'll just say, I believe that section 187 of the Criminal Code mandates that all documents that are related to a warrant under part VI of the Criminal Code, which includes video surveillance and wiretapping, be automatically sealed, so this is a backhanded move to ensure that all the warrants will never be released to our committee. It's a cover-up.

The Chair: Ms. Khalid.

Ms. Iqra Khalid: Chair, I take exception to everything that we do to try to balance out the work of this committee getting called a cover-up. That is absolutely not the case. What we're trying to do is to ensure that the RCMP, as they have been so forthcoming, are able to continue to be forthcoming with the documents that they provide in a manner that they can actually provide them. It's very unfair for Mr. Bezan to accuse us of cover-ups for a very small amendment like this, which only limits the scope of it so that we don't have to call commissioners in front of Parliament and hold them in contempt, or whatever other game the opposition may want to play.

The Chair: I see no further debate on the amendment, so I will begin again in hybrid. We'll do this in reverse, and I'll ask if there's anyone opposed to the amendment.

Mr. James Bezan: I'm opposed.

The Chair: I see opposition to the amendment. We'll ask the clerk to conduct a vote on the amendment.

There's a tie. I vote opposed.

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

The Chair: Now we're back to the original motion.

Is there any further debate on the motion? Seeing none, is there anybody opposed to the motion?

Ms. Iqra Khalid: I'm opposed, Chair.

The Chair: Okay, then, I will ask the clerk to conduct a vote on the motion.

There is a tie. I vote in favour of the motion.

(Motion agreed to: yeas 6; nays 5 [*See Minutes of Proceedings*])

The Chair: We have a couple of minutes, but I think, or I hope, we're done for now. We will be back this afternoon.

Actually, let me be clear about this afternoon. We have three witnesses who will be run together in a single panel. Depending on our timing and whether or not we exhaust members' desire to ask questions, we may have a bit of time at the end. I will put a hard stop on this at five o'clock, if I may, in case anybody has travel arrangements and whatnot and needs to be on their way by five.

With that, the meeting is adjourned.