HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

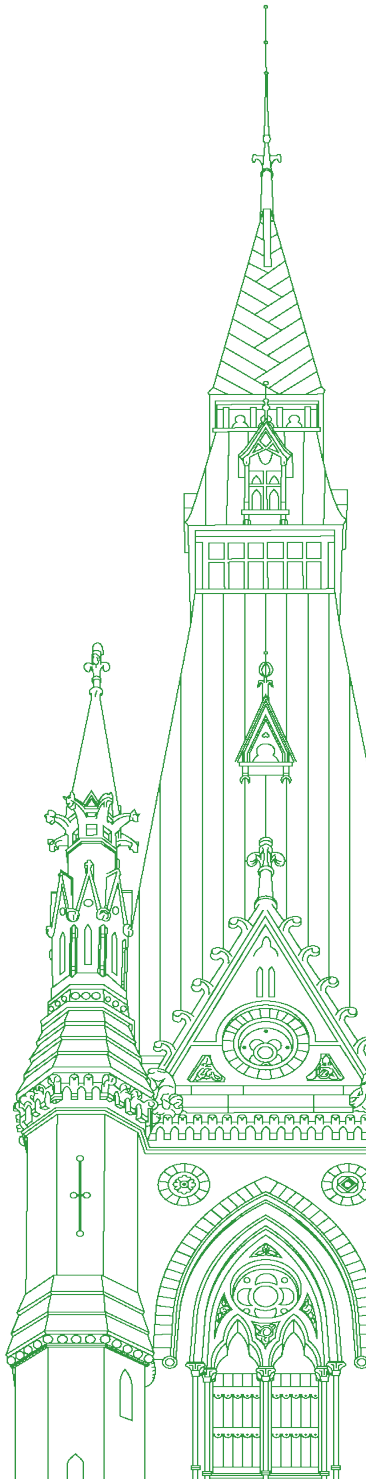
44th PARLIAMENT, 1st SESSION

Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 030

Monday, August 8, 2022



Chair: Mr. Pat Kelly

Standing Committee on Access to Information, Privacy and Ethics

Monday, August 8, 2022

● (1100)

[*English*]

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

Welcome to meeting number 30 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.

For members in the room, if you wish to speak, please raise your hand. Members on Zoom, please use the "raise hand" function.

The clerk and I will manage the speaking order as best we can, and we appreciate your patience and understanding in this regard.

I will introduce our witnesses for this panel this morning. We have with us from the Office of the Privacy Commissioner of Canada, Philippe Dufresne, Privacy Commissioner of Canada; and Gregory Smolynec, deputy commissioner, policy and promotion sector.

We will now begin the opening remarks. The floor is yours.

Take it away, Commissioner Dufresne.

Mr. James Bezan (Selkirk—Interlake—Eastman, CPC): I have a point of order, Mr. Chair.

The Chair: I'm sorry, there's a point of order.

Go ahead, Mr. Bezan.

Mr. James Bezan: When the hammer drops, there are supposed to be no cameras in the room.

The Chair: Correct, thank you. I think we have co-operation there.

With that, take it away, Commissioner.

Mr. Philippe Dufresne (Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada): Good morning Mr. Chair and members of the committee.

I am pleased to be here today to assist the committee in its study of the device investigation tools used by the RCMP. I am accompanied by my colleague Gregory Smolynec, deputy commissioner, policy and promotion branch.

This study follows media reports and a response to a question on the Order Paper confirming that the RCMP was using technical tools to obtain data covertly and remotely from targeted devices, subject to judicial authorization. The response and media reports also indicated that the RCMP had not consulted my office prior to using these tools.

[*Translation*]

As you know, as the Privacy Commissioner of Canada, I am responsible for the protection and promotion of the privacy rights of Canadians in the public and private sectors. My office does so by investigating complaints, providing advice to government departments and private sector organizations, reporting publicly on compliance with privacy laws, and promoting public awareness of privacy issues.

When I appeared before you in June to discuss my proposed appointment as Privacy Commissioner, I indicated that I would have as my vision the following three elements: privacy as a fundamental right; privacy in support of the public interest; and privacy as an accelerator of Canadians' trust in their institutions and in their participation as digital citizens.

● (1105)

[*English*]

Applying these elements to the committee's study generally, I would say the following.

Privacy as a fundamental right means that all institutions, including the RCMP, should have privacy as a key consideration when designing and deciding to use any technology that could have adverse impacts on the privacy of Canadians.

Privacy in support of the public interest means that by considering privacy impacts at the front end and by consulting with my office, organizations can prevent privacy harms at the outset and indeed improve the tools that will be used to further the public interest, whether it be the prevention of crime, the protection of national security, or the advancement of Canada's competitiveness. Privacy and the public interest go hand in hand, they build on and strengthen each other and Canadians and their institutions should not have to choose between one or the other.

Privacy as an accelerator of Canadians' trust in their institutions and in their participation as digital citizens means that when organizations such as the RCMP consider privacy impacts at the front end and are seen to be doing so, this generates trust and reassures Canadians about the necessity of the tools and the measures put in place to mitigate privacy impacts and ensure proportionality between the measures and the objectives.

[*Translation*]

In terms of specific background to your study, I would start by saying that the Privacy Act does not require the RCMP or any government institution to prepare privacy impact assessments, or PIAs, for my consideration, but the Treasury Board requires it in its policies. I hope to see this included as a binding legal obligation in a modernized version of the Privacy Act.

As you know, the RCMP recently indicated that it had put in place a program to use on-device investigative tools, or ODITs, and other methods to obtain data covertly and remotely from targeted devices. The RCMP confirmed that these tools could collect private communications such as texts and emails sent or received from the device, documents and media files stored on the device, as well as sounds within range of the device and images viewable by the cameras built into the device.

The RCMP has also stated that the use of these tools is subject to judicial authorization. My office was not informed of, or consulted on, this program prior to its implementation or since. After learning about this through the media in late June, we contacted the RCMP for more information, and the RCMP has since scheduled a demonstration for my officials in late August. In its response to the question on the Order Paper, the RCMP indicated that it began drafting a PIA in relation to these tools in 2021, but we have not yet seen it.

[*English*]

Once we receive the PIA, we will review it to ensure that it includes a meaningful assessment of the program's privacy compliance and measures to mitigate privacy risks. We will also review it to ensure that any privacy-invasive programs or activities are legally authorized and necessary to meet a specific need, and that the intrusion on privacy caused by the program or activity is proportionate to the public interest at stake. This would require the RCMP to consider whether there is a less privacy-intrusive way of achieving the same objective. If we find shortcomings in terms of privacy protections, we will provide the RCMP with our recommendations. We would expect them to make the necessary changes.

In conclusion, I would reiterate my hope that the timely preparation of PIAs be made a legal requirement in a modernized version of the Privacy Act. Doing so would recognize privacy as a fundamental right, support the public interest and generate necessary trust in our institutions, such as the RCMP, who are doing vital and important work for all Canadians.

I would now be happy to answer your questions.

The Chair: Thank you.

For the first round of questions we have Mr. Kurek.

You have up to six minutes. Go ahead.

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

Thank you, Commissioner, and congratulations. I know that the last time you were before this committee, it was expected that you would be appointed, so congratulations on that appointment. I'm sure it's been a busy summer for you.

You referenced in your opening remarks how one of your priorities as commissioner is viewing "privacy as a fundamental right". Certainly, with the Order Paper question, there were some concerns about the way the RCMP and the government approached the procurement of this software. I'm wondering if I could hear your opinion on whether or not you would see the government sharing your opinion that privacy is a fundamental right in the way this process seems to have been carried out.

● (1110)

Mr. Philippe Dufresne: I know that the Department of Justice has issued a paper recommending proposed modifications to the Privacy Act in a modernized version, as this committee has done as well. One of those goes to the preamble and strengthening the language in the preamble to highlight the fundamental importance of privacy to the dignity and rights of Canadians.

What I would say is that seeing this as a fundamental right, all institutions should have it as top of mind. It should be a culture of privacy. It should be privacy by design so that when thinking of new tools, new public interest opportunities, priority is given to considering the impacts on privacy.

Mr. Damien Kurek: I found it interesting when you shared a little bit of the timeline regarding the RCMP's response to basically being called out on this with this Order Paper question and the revelations. Do you find it suspect or curious that it was only after having this information go public that it seems they would have been more forthcoming with their privacy obligations?

Mr. Philippe Dufresne: What I will say is that the impact of this type of information coming out in the public through media reports or questions can raise questions and can raise concerns. I think from a trust standpoint and generating confidence, it would be far preferable that privacy impact assessments be done at the front end, that my office be consulted, and that this can be conveyed somehow to Canadians so that they are reassured that there are institutions there, such as my office, to provide advice and to make sure that privacy is top of mind.

Mr. Damien Kurek: Just to clarify, especially when it comes to law enforcement, we have heard, and I'm sure we will hear, about the operational realities of an investigation. Does your office have protocols in place to make sure that things like investigations and the integrity of those things could be protected?

Mr. Philippe Dufresne: When we work with organizations, we ensure that the information is treated appropriately in terms of confidentiality and security. From my standpoint, as I stated, privacy is not an obstacle to the public interest. They go hand in hand. They strengthen each other.

Mr. Damien Kurek: Thank you very much, Commissioner.

I know that your office and a number of the other offices that report to this committee do some proactive work to look at how government is fielding their various areas of responsibility. I'm just curious; has your office discussed or looked at software such as Pegasus or other types of spyware and their potential to jeopardize the rights and human rights of Canadians? Is that something that your office has looked into outside of the context of this study that we're undertaking now?

Mr. Philippe Dufresne: I know that this has been discussed in terms of the appearance of my predecessor at this committee with regard to facial recognition technology. There were questions asked about that. To my knowledge, this is not something that is used by government institutions, but this type of technology is the type of technology that to my mind should be looked at very carefully from a privacy standpoint to ensure that its impacts are known and mitigated.

Mr. Damien Kurek: Just to clarify, your office has not undertaken an assessment of the use of software like Pegasus or other types of spyware and their impact on the privacy of Canadians.

Mr. Philippe Dufresne: No, we have not, but in the context of this matter, we look forward to receiving the PIA and information from the RCMP—not with Pegasus, but with the type of tools that are being used in this context.

Mr. Damien Kurek: Are you aware of, outside of the information that was provided in response to the Order Paper question that's been referenced, other entities in government that have used this throughout the last number of years, especially with the rapid evolution of types of technology like this? Are you aware of whether this type of technology has been used in the past and other privacy assessments have been done?

Mr. Philippe Dufresne: I'm not aware of other types of technology or privacy assessments. Our office has been involved in reviewing the facial recognition technology. It has been involved in Clearview and the use of images and an investigation in terms of cell site simulators—these types of technology. When we are involved, we look at the privacy impacts. Public interest may require the use of these tools, but we look at making sure the safeguards are there to minimize and to ensure that it's proportional.

Mr. Damien Kurek: In my last few seconds here, can I ask whether your office has been in touch with any provincial counterparts on these or related matters regarding the use of technologies during law enforcement investigations?

● (1115)

Mr. Philippe Dufresne: In the context of facial recognition technology, there was coordinated work with provincial privacy commissioners. A joint statement was issued on recommended principles in these matters.

Mr. Damien Kurek: Has there been any work—

The Chair: You're out of time, Mr. Kurek.

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

The Chair: We will now go to Ms. Hepfner.

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

Through you, I'd like to thank the Privacy Commissioner and Mr. Smolynec for being here to answer our questions today.

I would like to take you back through a little bit of the timeline. I think you said that you understood about the RCMP's use of technology in June, and then you got an update from the RCMP just this month. Have you gotten some information already from the RCMP about their use of technology that can be used to spy on people's cellphones?

Mr. Philippe Dufresne: Not at this time; we were made aware of its use through the media and the question on the Order Paper at the end of June. We reached out to the RCMP. They are aiming to provide us with information at the end of August. It will be coming this month, but it hasn't come yet.

Ms. Lisa Hepfner: Okay.

From what you know of the RCMP's limited use of technology in some investigations, do you have concerns about how it was being used? Can you explain any privacy concerns or other concerns you have about a violation of people's rights under the charter?

Mr. Philippe Dufresne: Well, we have not received detailed information in terms of the context and the use. That's what we look forward to receiving and to providing advice on with the facts. I think what I could say at a high level is that, on the one hand, these tools appear to be potentially highly intrusive in terms of their capabilities to gather information. On the other hand, they are also subject to an extensive regime in terms of judicial authorization and conditions. We will look at those two aspects to see the intrusiveness of the tools but also the safeguards, including the fact that they are, if they are, and the extent to which they are subject to judicial authorization and the criteria and notification—the elements in terms of the Criminal Code. We're going to look to see if, given the evolution of the technology and the capabilities, there should be more in terms of safeguards, whether it be with respect to retention policies or otherwise.

These are the things we're going to be looking at once we have the briefing and the more detailed information, as we would have done and as we would do in the context of any program where a PIA would be done.

Ms. Lisa Hepfner: Thank you.

You mentioned that there should be some updates to the Privacy Act that should include this under its purview. I'm wondering if you can give us a little bit more detail about how that legal framework should look.

Mr. Philippe Dufresne: Sure. Currently, there's no legal obligation on departments or the RCMP for doing this. There is a policy from the Treasury Board and there's a directive. Those policy instruments require that PIAs be done when there's a new program or new use that could potentially be having an impact on the privacy of Canadians. There's a requirement that my office be notified early enough so that we can provide meaningful input. The idea, again, is to reassure Canadians, and also to ensure that the information and advice is there.

But we see situations like this one, where this is done very late, after the tools have been used for some time, so we're not in a position where we can address or prevent. We're in a reactive mode. Our advice and recommendation, or my hope, is that this be made a legal obligation in the Privacy Act, because then there hopefully would be more timely compliance with this requirement.

Ms. Lisa Hepfner: Is the RCMP required to consult with you before starting the use of technology like this, given that there are several layers of judicial authorization needed for them to use the technology?

Mr. Philippe Dufresne: Under not a legal obligation but under the policy documents of the Treasury Board; this is something that's not legally required but is more internal. The sanctions could be imposed by the Treasury Board itself...or removal of delegation or these types of things, but there is certainly in this policy the sense that my office should be notified and that a PIA should be done in high-risk situations where the tools can have an impact on privacy.

The fact that there's a judicial authorization regime doesn't remove the need to do a PIA, but it's an important element that would certainly be looked at and considered in a PIA as a mitigation measure.

● (1120)

Ms. Lisa Hepfner: And you would like to see it become a legal requirement that your office be consulted.

Mr. Philippe Dufresne: That the PIA be done would be the legal requirement and that my office be consulted in appropriate cases; again, there may be situations where you have to manage the risk at play. There's also the sensitivity of the information. Situations have to be looked at on their facts.

Our recommendation is that if it were a legal obligation, there would be more compliance. Maybe it would help organizations ensure that they do it, that they have the resources to do it and that they're coordinated enough to do it. I understand that organizations have a lot of pressure and have a lot of things they have to bear in mind. I'm very sympathetic to that. I think having it as a legal obligation is sometimes helpful, because it focuses the attention on that.

The Chair: Thank you.

With that, Ms. Hepfner, you are out of time.

[*Translation*]

Mr. Villemure, we now go to you for six minutes.

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

Commissioner, like my fellow members, I want to congratulate you on your recent appointment.

Let me say, from the outset, that the purpose of this study is not to carry out a witch hunt but, rather, to see whether improvements are needed, whether a legislative framework or public policy is needed to protect Canadians. Respect for fundamental rights, public trust and the public good are all things we are trying to achieve here.

Thank you for being with us this morning.

There is no denying how quickly technology moves, sometimes faster than legislation. Nevertheless, other countries, or the European Community, has begun looking into spyware.

What can you tell us about a government entity's decision to use or not use spyware?

Mr. Philippe Dufresne: A government entity's use of spyware raises privacy concerns right off the bat. That doesn't mean that it won't be allowed in situations where it's appropriate. As I said earlier, privacy is not an obstacle to the public interest, but it always has to be taken into account. Privacy is a fundamental right and needs to be taken into account. It's a matter of human dignity.

You're right about how quickly technology is moving, and tools are becoming more and more sophisticated. This isn't the same as just intercepting a conversation on a landline; smart phones hold a wealth of information.

The approach we advocate is taking privacy into account from the get-go, especially given the potential for technologies to be more and more privacy-intrusive. Also important is the ability to properly weigh the risks and the necessity of using the tool.

My office and this committee recommended necessity and proportionality as criteria. That is not to say that the tool can't be used. Perhaps it can. Perhaps, in this case, that balance was achieved, but it's important to make sure. Those checks and balances not only protect privacy, but they also reassure Canadians that privacy is being respected.

Mr. René Villemure: A sense of security is indeed very important in this situation.

On its own, a tool isn't moral or immoral. The problem really has to do with how it's used. Admittedly, these tools are extremely intrusive. They can be installed on people's phones unbeknownst to them.

I think it's your office's job to review and verify assessments that may be done upfront.

Do you think the RCMP or similar organizations need oversight when it comes to assessing their practices?

Currently, they do their own assessments. If they tell us that it's appropriate to use this or that tool, I'm willing to believe it, but self-assessment has its limits.

What do you think?

Mr. Philippe Dufresne: This afternoon, you'll be hearing from RCMP representatives. I think they will highlight the fact that these tools are subject to oversight under part VI of the Criminal Code. In its response, the RCMP said that the use of these types of tools was subject to judicial authorization. That's an important aspect.

That oversight comes down to criteria set out in a section of the Criminal Code for the purpose of protecting privacy while allowing criminal investigations to take place.

What we are saying is that, when these tools are new, very powerful and potentially intrusive, it's important to carry out privacy impact assessments, even if judicial review mechanisms are in place. There is a system that has that requirement, but it's not a legal one. It's the system that was put in place pursuant to the Treasury Board policy. My office asks departments to ask these questions and to document the information.

At the end of the day, the results may show that, while these tools are certainly intrusive, they are necessary given the difficulty of conducting the investigation and the lack of alternatives. It's not about choosing between the public interest and privacy; it's about ensuring respect for both, but it has to be done in a way that builds trust. It's better to carry out assessments at the front end so that the use of these tools doesn't come to light in a news report or in response to a parliamentarian's question. This kind of situation can be avoided by conducting assessments first and by consulting my office when appropriate.

● (1125)

Mr. René Villemure: Now it feels as though there's been a breach of trust.

Currently, a number of bills relate to privacy, including Canada's digital charter.

I worry that all these bills have gaps. Do you have a recommendation that might help?

Mr. Philippe Dufresne: Parliamentarians, my office and stakeholders need to ask questions and examine the possible repercussions these tools have on privacy.

You're right: there are a number of bills and initiatives. Organizations need to address privacy considerations in their plans and activities, and parliamentarians need to do the same when it comes to bills. My office is here to provide the committee with advice on legislative measures.

Mr. René Villemure: Do you think we need a moratorium on spyware right now, so we can take the time to really examine things?

Mr. Philippe Dufresne: We said the same thing in relation to facial recognition technology: it's important to consider the safeguards in place. That includes the requirement to obtain judicial authorization before using spyware.

My priority is to determine what the repercussions and implications of using the tools are, and to make recommendations based on the information provided by the RCMP. We hope the RCMP will follow through on our recommendations, and that's what we expect.

Mr. René Villemure: Thank you.

[*English*]

The Chair: Thank you.

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

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

Already, some very important points have been raised. Hopefully, they will help guide us in future discussions on balancing Moore's law and the advancement of technology with legislation and, quite frankly, a workforce that may not be as up to date on the technology, to be able to provide adequate insight on its proportionality.

Mr. Dufresne, you mentioned that you're looking to see the privacy impact assessment as a legal requirement. Can you take a brief moment to expand on why it would be important for your office to provide oversight on the basic functions of this rapidly increasing and expanding use of technology?

Mr. Philippe Dufresne: Absolutely.

Privacy impact assessments, in my mind, are an important tool for a culture of privacy, for a culture where privacy is top of mind. We are designing tools for organizations that are meeting many obligations and facing pressures. Time is limited for decision-makers and I understand that, but having that framework is about getting into this habit of asking questions: What is the impact on privacy? How large is it? How necessary is it? What is my purpose? Why do I need this information? Do I need as much? What are the safeguards we're putting in? All of this risk assessment, the identification of mitigation tools and the identification of proportionality create a culture of privacy and a culture of privacy by design, and in the ideal scenario, it means that my office doesn't need to be involved—or very little—because we're informed of it; we're notified. We then look at it and we're satisfied, or we provide some advice. It doesn't give rise to situations where there is a complaint, a concern or a sense of mistrust, or where questions are being asked.

This is good, in my mind, for everyone. It ensures the protection of privacy for Canadians, ensures organizations can achieve their goals and ensures there's trust in society so Canadians can feel they can use these tools and participate as digital citizens.

● (1130)

Mr. Matthew Green: When you talked about strengthening the language of privacy as a culture, you mentioned strengthening fundamental rights in the language of the preamble. Just so that I'm clear, is a preamble legally binding in legislation?

Mr. Philippe Dufresne: It's not legally binding to the extent that a section of the act is, but it would be looked at in identifying the purpose of the act and in identifying sections of the act. The preamble is very helpful, so we would look to—

Mr. Matthew Green: But it's not legally binding.

Mr. Philippe Dufresne: It's legally binding in the sense that it's going to be interpreted by courts in terms of how the statute and the sections of the act will apply. However, you would want sufficient protection in the sections themselves. If there is a lack of clarity or some elements need to be given some nuances, the preamble will assist in highlighting what the intention was.

Mr. Matthew Green: Has there been any contemplation by your office on what legally binding language might look like in the Privacy Act? I ask because quite like my good friend Mr. Villemure, I'm interested in seeing the fruits of this labour over the next two days result in recommendations that will hopefully strengthen the new Privacy Act.

Before you answer that, I want to reference the time we spent on mobility data tracking. That was a culture referencing the Treasury Board. It has this language within it, but we had a department that went beyond the scope of the Treasury Board's directives and had this committee spending a considerable amount of time contemplating that use.

Help me close the gap between suggestions, culture and preamble, and strong legal requirements for privacy.

Mr. Philippe Dufresne: In the context of this study—and there was the study on mobility data—there was a study that this committee did in 2016 on overall Privacy Act reform. There were a number of recommendations. The one that is very relevant here and that I'm reiterating is the one about having, in the act, a section requiring that organizations prepare privacy impact assessments when they are designing—

Mr. Matthew Green: I want to jump in on that. We spoke briefly before the meeting, and you know that I have been trying to champion the duty of candour. I would put to you, given your past roles, that you know better than most how serious and how important Parliament is, as the grand inquisitor of the nation, in ensuring there is civilian, democratic oversight of our institutions. However, it seems like—in fact, I believe there's been judicial comment on this—CSIS and the RCMP have a bit of a cavalier approach to Parliament.

Do you think privacy assessments should also be made readily available to this committee? We could help offset some of the unnecessary time we might spend in investigating these things if there were a bit more of a proactive duty of candour within this particular committee.

Mr. Philippe Dufresne: This idea is similar to why my office should be receiving notifications of these privacy impact assessments. There was a recommendation made, I believe by this committee, on not only requiring PIAs but also requiring reports, or more fulsome reports, on privacy management initiatives and privacy steps.

This information can be made available publicly, or if there is some issue about public information, it can be made available to the proper entities, such as my office and this committee. If information has to be confidential, there are tools for that, but it is important that the proper bodies, including this committee and the House, have this information. Again, it generates this notion of trust in that questions may not need to be asked if you have this information provided on a proactive basis. That allows the organization to fulfill its important public interest without having to answer these questions after the fact.

Mr. Matthew Green: Thank you.

The Chair: Thank you.

Now we'll move to Mr. Williams for up to six minutes.

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

I'll follow my colleagues' questions and I'll also amplify them. Thank you very much for attending and being here today.

Can you hear me? Do I have five minutes?

● (1135)

The Chair: Yes.

Mr. Ryan Williams: Thank you.

I want to walk back a little bit on how your office became involved today and why we're here.

Did you hear about this technology only through the media, or were there other ways you heard about how this was occurring?

Mr. Philippe Dufresne: We heard about this from the media.

Mr. Ryan Williams: Do you have any more information in your office at this point, or is it just that you're going to get information at the end of August?

Mr. Philippe Dufresne: The information that I have is the information that I have from the media reports. It's also from the RCMP's answer to the question on the Order Paper, so there is more information there.

I know that there will be a more fulsome briefing to my officials at the end of August, but I don't have more information than that today.

Mr. Ryan Williams: Did you formally request more information at this time or at any time prior to her hearing about this in the media?

Mr. Philippe Dufresne: As soon as we heard about it in the media on June 27, we reached out to the RCMP. I believe on June 30 we made the request for the meeting, and the meeting will take place at the end of August.

Mr. Ryan Williams: Did you just ask for a meeting and no other information at the time?

Mr. Philippe Dufresne: What I understand is that we asked to be provided with information about this initiative, these tools, and a briefing on those tools. I don't know if there's more information.

I expect that we're going to receive enough information so that we can provide meaningful input on this. I expect that we will receive the PIA as well.

Mr. Ryan Williams: Have you asked for the PIA?

Mr. Philippe Dufresne: We've been informed that the PIA was done in 2021, and this is something that we're going to want to see. I don't know if we're going to see this at the end of August, but this is something that we will want to see.

Mr. Ryan Williams: Going on some of the last testimony, you mentioned that the PIA's are non-intrusive, that they're very private themselves.

Have you done a PIA on the RCMP and other technologies in the past?

Mr. Philippe Dufresne: What I know is that the office was involved in reviewing the facial recognition technology and the Clearview AI. We also had an investigation on the use of cell site simulator data.

I don't know if my colleague has more information on PIAs that would have been proactively shared and discussed with us.

Dr. Gregory Smolynec (Deputy Commissioner, Policy and Promotion Sector, Office of the Privacy Commissioner of Canada): There have been other PIAs submitted by the RCMP historically in the past.

Mr. Ryan Williams: Have they always given fully what your office needed when you've asked for them?

Dr. Gregory Smolynec: Typically, it's not unusual in a PIA submission that we would request additional information upon receipt of the PIA; we'd ask additional questions. It's a little bit of an interim process where we may ask for supplementary information or documentation as part of our review of a PIA. That happens quite frequently.

Mr. Ryan Williams: With regard to your office and your knowledge, when it comes to all of this new technology that we're using, are you aware of who approves this information? Is it the RCMP themselves, or are any offices of the government involved at all, for instance, is Public Safety, etc., involved in any procurement of that technology?

Mr. Philippe Dufresne: I'm not sure of the internal workings. This is a question that should be properly asked of the RCMP.

I've seen the information they gave and the question on the Order Paper.

Mr. Ryan Williams: When we talk about this technology—and we went through this with your predecessor before with regard to facial recognition and cellphone mobility data—does it concern you that a general warrant with this kind of technology is all that's necessary to remotely access someone's phone, and the microphone or camera?

Mr. Philippe Dufresne: Again, I will want to know the details from the RCMP in terms of which warrant and which authority they are using. If it is part VI of the Criminal Code, there are more safeguards there in terms of authorization and notification to the person after the fact. This is going to be part of what we look at to see if it's enough and, if this is used, if it's this one, if we need to strengthen it with other means, but part VI in the Criminal Code does have a number of safeguards built in.

Mr. Ryan Williams: We know that this technology has been used in the U.S., and it's no longer allowed to be used in the U.S.

This will be my last question, Mr. Chair.

Would you have concerns on its use in general just from knowing what you know right now, and what would those concerns be?

Mr. Philippe Dufresne: My concern is making sure that this type of technology is looked at from a privacy angle and that it be looked at carefully to ensure that it doesn't go further than it needs to in order to achieve the necessary public interest at play.

This is something we'll be able to do once we see the details of the specific tools as well as the uses, the purposes and the safeguards.

● (1140)

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

The Chair: Thank you.

Ms. Khalid, you have up to five minutes.

Ms. Iqra Khalid (Mississauga—Erin Mills, Lib.): Thank you very much, Chair.

Thank you, Monsieur Dufresne, for being here today.

I will start by going back to something you said that I want to clarify. I believe you said that, to your knowledge, there is no Pegasus-like tech that is being used, that you're aware of, by government departments. Is that right?

Mr. Philippe Dufresne: I think Pegasus itself; I think I was referring to this program, and to my knowledge it is not used by any government agencies.

Ms. Iqra Khalid: Sir, you have a lot of experience. On a world scale, where does Canada place in its protection of the privacy of Canadians from mass surveillance or the use of Pegasus-like technology in surveilling Canadians? Where does Canada stand in the world?

Mr. Philippe Dufresne: I think Canada has a number of safeguards. The role of my office is to ensure that we can make them stronger and to promote making them stronger. We've called for law reform for the Privacy Act to modernize it so that it catches up to new technology. There is Bill C-27, which is currently before the House in terms of private sector privacy.

We value privacy as Canadians, and I think it's something that has to be top of mind. That's why I say that privacy is a fundamental right. It has to be so. It has to be seen as such. It is not an obstacle to the public interest. It has to be there. It has to work with the public interest, but it has to be something that we communicate and we address to build trust for Canadians.

I think we have a strong system. I think it could be stronger. I think it's important that it be world class and that it be the best system in privacy. It's a fundamental right, and it's fundamentally important for Canadians.

Ms. Iqra Khalid: Thank you.

You just mentioned the use of such surveilling technologies by private organizations. I know that in the news we heard recently about the Awz group, which former prime minister Stephen Harper has been deeply involved with. There's technology such as Corsight, which uses facial recognition software, or viisights and their behaviour recognition software.

Are you concerned about how those technologies being developed are being used by private companies, and whether we should be doing more? You just mentioned Bill C-27 as well. Perhaps you could expand on that.

Mr. Philippe Dufresne: I think it's important for both the private sector and public sector that we have modernized legislation that treats privacy as a fundamental right, that does so while advancing the public interest, and that does so by generating trust. There will be some different considerations in terms of necessity and proportionality in terms of ensuring that whatever tool is used is warranted and is legitimate to goal.

In terms of the public sector, there will be a necessity that will often be at a higher level. If you're talking about the public interest, national security, prevention of crime and so on, they're distinct situations, and they have to be looked at in context.

Ms. Iqra Khalid: Thank you.

Lastly, I want to go down this path. We know that over the past number of years, the RCMP has investigated, for example, members of Parliament. That is part of the motion that is before us. Obviously, the work you do as Privacy Commissioner impacts all government departments. It impacts the House, and it tries to protect the privacy of Canadians. Where do you see that balance between the role that the RCMP plays in balancing privacy and security of Canadians versus the role that you play in ensuring that privacy is protected and also that justice is done, and is seen to be done as well, in an efficient manner? What are your thoughts about that?

Mr. Philippe Dufresne: As the Privacy Commissioner, my mandate is to promote and protect the privacy rights of Canadians in the public and the private sector. That's the mission that I have and that my office and my colleagues have. But my vision would be that we have a culture of privacy in Canada throughout the whole of government, and that whatever organization, whatever department, including the RCMP, has privacy as a consideration.

The RCMP has its own mission and its own mandate in terms of protecting Canadians. They can talk about it more eloquently than I can, but I concluded my remarks by describing it as being vital and important to Canada. It's of fundamental importance. My goal is that, by doing so, they nonetheless have privacy as top of mind. I think that is doable. I think that strengthens privacy, which is a fundamental right, but it also strengthens the mission of organizations, in this case law enforcement, in protecting Canadians, because it generates trust and ensures that Canadians will know what they can do and what's being done. I think that ultimately helps the RCMP in its mandate.

● (1145)

Ms. Iqra Khalid: Lastly—

The Chair: Thank you.

No, I'm sorry, Ms. Khalid; you're out of time.

Ms. Iqra Khalid: Thank you, Chair.

[*Translation*]

The Chair: Over to you, Mr. Villemure for two and a half minutes.

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

Commissioner, part VI, the part of the Criminal Code you just mentioned, comes up a lot in the documents provided by the RCMP. When I read the documents, I got the sense that part VI was something of a replacement for the Office of the Privacy Commissioner.

What are your thoughts on that?

Mr. Philippe Dufresne: Thank you for your question.

The fact is it doesn't replace the Privacy Commissioner. They are two different things. Part VI sets out the conditions in which police can use the tools. It stipulates the obligation to obtain authorization from a judge, the obligation to give notification and various other conditions. That is very important.

One thing is for sure. If the use of a tool was not subject to such obligations or a regime like this, there would be even fewer mechanisms to limit that use. A tool that is used across the board for everyone will certainly be handled differently than one that is used specifically for the purposes of an investigation. However, that does not relieve police of the necessity to assess the potential privacy repercussions when they plan to use new tools. That is why my office views those assessments as necessary, and we can contribute to the process by providing advice and an opinion on the issue.

Perhaps we will come to the conclusion that the assessment mechanism is adequate and come away reassured. The police could then tell the public that the tool had been scrutinized, and Canadians would be reassured. Perhaps we will conclude that the mechanism is quite good but has a few gaps given how quickly technology evolves. The regime would then need to be strengthened, and new criteria or safeguards added. All of that is possible, but it won't automatically flow from part VI, and that's where my office comes into the equation.

Mr. René Villemure: Part VI does a good job of establishing limits, but your office provides additional oversight and a different perspective, one that is needed.

One of my fellow members brought up the Treasury Board's directives. They don't carry the same weight as the law—there is no disagreeing with that.

I gather from your previous comment that these obligations should be prescribed in the act instead of set out in an administrative directive that can change at any time.

Is that correct?

Mr. Philippe Dufresne: In my view, that's the thing to do. An administrative directive can always be changed. An act can also be changed, but it's obviously a more cumbersome process.

Conducting the assessments is what matters. Given the benefits to Canadians and the organization of conducting the assessments, making them a legal obligation, I think, will incentivize people to do them. When decision-makers have multiple obligations to meet at the same time, they will obviously prioritize those that—

[*English*]

The Chair: I'm sorry, Commissioner; I'm going to have to go on to Mr. Green. It's tough, but sometimes I'm just not going to be able to let questions—

[*Translation*]

Mr. René Villemure: Thank you very much.

[*English*]

The Chair: —go fully or the answer go too long when a question is posed right at the very end of the round.

Go ahead, Mr. Green.

Mr. Matthew Green: Do you believe that the use of technologies like this by law enforcement has the potential to violate rights guaranteed by the Charter of Rights and Freedoms?

Mr. Philippe Dufresne: Well, the Charter of Rights is there, and I think it can be raised in appropriate cases if there's a violation. I think that the regime is there and the protection is there. This is something that would be raised before courts and would be decided by courts.

What I would say in terms of my mandate as the Privacy Commissioner is that these technologies have the potential of having impacts on privacy, so they need to be looked at from that standpoint. There is a regime that allows that, and it is the regime of the privacy impact assessments, and I would hope that this be made a legal obligation and be done early enough in the process so we can course correct, if needed, as opposed to doing it long after it's been started.

● (1150)

Mr. Matthew Green: Thank you.

I know that you mentioned that you'd like to see frameworks in place to ensure that technologies don't go further than they need to, and I'm not sure if you are aware of the document submitted by the RCMP on a warrant, which is like a sample warrant.

Are you familiar with the matter for the application of general warrants by Justice Bertha Wilson? Did you have a chance to look at that?

Mr. Philippe Dufresne: I'm not sure that I am.

Mr. Matthew Green: I'll reference it for you, just the top sentence, which says, “When oral communications have been intercepted using an ODIT, the monitor who subsequently reviews the communication must cease reviewing the communication as soon as the monitor determines that no person in paragraph 3a is a party to the communication”. It sets a parameter.

The challenge that I have with the cavalier nature of law enforcement—you referenced stingray technology where they're mass intercepting communications from everybody and then deciding which ones they'll use—is who reviews their use? Once this warrant is granted and surveillance has begun, what mechanisms are in place to ensure that the RCMP are adhering to the terms of this warrant?

Mr. Philippe Dufresne: That's right; this is what we want to be looking at, and these are questions you may want to ask the RCMP when they appear before you. How does the regime work? How well does it work? There is judicial authorization, and there is follow-up that can be done there. There's notification after the fact—

Mr. Matthew Green: Just quickly, before my time is up, do you have anybody in your office who you feel has the technical knowledge to deal with the emerging technology at pace with the legislation?

The Chair: Your time is up. We have time for a yes-or-no answer and then we have to move on.

Mr. Matthew Green: Could he perhaps prepare that in writing for the committee?

The Chair: You may request so.

Mr. Philippe Dufresne: We can provide information to the committee on our technical unit.

The Chair: Thank you.

With that, we will go to Mr. Bezan.

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

I want to thank the Privacy Commissioner and the deputy commissioner for being with us today. I think this is an important discussion.

I just want to go back to what you said earlier in answering questions from Ms. Khalid, that Pegasus is not used by other government departments. How do you know that, when the RCMP never disclosed proactively that they were using on-device investigative tools? How do you know that CSIS, CSE, CBSA and National Defence are not making use of this type of technology?

Mr. Philippe Dufresne: Right; what I perhaps should have said is that I'm not aware of any government entity using it. I don't know for a fact that they're not, but I don't have confirmation—

Mr. James Bezan: So really, this is about a lack of transparency by the government, because they haven't been disclosing this information to you proactively. That's why we need to have the privacy impact analysis embedded in the Privacy Act legislation, so that all departments are obligated to do these impact analyses and request the advice of your office to ensure that they are compliant.

Now that you know that the RCMP have deployed this technology in the past, have you reached out to other government agencies that are responsible to you on whether or not they're using other Pegasus-type ODIT?

Mr. Philippe Dufresne: No, we have not. We reached out to the RCMP after this matter became public. We would expect the government departments to have the onus on reaching our office and advising us if they are using tools. That's the expectation.

Mr. James Bezan: You wouldn't be interested in actually asking them directly, in your role as commissioner, if they will disclose that they use on-device investigative technology?

Mr. Philippe Dufresne: We could reach out to them in our exchanges, but what's important, I think, is that the obligation rests on departments themselves to notify my office if they are using these tools. I wouldn't want to create an expectation that unless we proactively ask all organizations they don't have to provide us with the information. I think it's important that this is how the directive and the policies of Treasury Board are designed. The onus is on the organizations to advise the Privacy Commissioner of the use of those tools, and I would expect them to do so.

● (1155)

Mr. James Bezan: You know, as Conservatives we do believe that we want to make sure that police agencies and our national security and criminal investigations have the appropriate tools to do this as long as charter compliance is in place and privacy rights are protected. How do you feel about the unintended consequences? They may have a warrant to turn on a cellphone and monitor the data or the video of conversations happening involving a person of interest, but what about the other Canadians who might be around that device and have their privacy violated as well? How do we balance that off?

Mr. Philippe Dufresne: That is exactly the type of question we would be asking in terms of looking at a PIA. This is the type of approach that I would call a culture of privacy. What is the impact on the privacy of Canadians? Are you going further than you need to? You may well need to do it to investigate one individual, but are you using a tool that's going to be gathering information about other individuals? Is that necessary? Can that be avoided? Can that be mitigated?

This is part of the context we would want to look at to see if it's minimally intrusive from a privacy standpoint.

Mr. James Bezan: Is there a responsibility across government agencies and departments to ensure that they respect the charter, where they are prohibited from spying on Canadians? This is spyware. They cannot directly or indirectly spy on Canadians without proper warrants. Do you believe the current warrant system we have in place is modern enough to deal with the spyware that's out there now?

Mr. Philippe Dufresne: Well, this is why we need this information. This is the question that we will be asking when we receive the briefing on the information, to see whether, given this new technology, the safeguards are sufficient, or whether we have to make recommendations to make it safer from a privacy standpoint. These tools may well be needed, but do they have an impact from a privacy standpoint that is greater than what is warranted given the purpose?

This is an important question. This is the central question, to my mind, when doing a PIA, looking at the purpose and looking at the impact.

Mr. James Bezan: Thank you.

The Chair: Thank you.

Now we have Mr. Bains for five minutes, please.

Mr. Parm Bains (Steveston—Richmond East, Lib.): Thank you, and thank you to our guests for joining us today.

According to the RCMP's response to the Order Paper question and the questions that the Office of the Privacy Commissioner raised concerning the covert access and intercept team, what were those concerns?

Mr. Philippe Dufresne: We did not raise concerns with respect to the specific use of tools in this instance because we have not been consulted on them yet. We will be consulted on this at the end of August.

I believe the reference is made to some of the other investigations that took place by my office of the cell site simulators and the Clearview AI, which was the use of facial recognition images of citizens.

There has been engagement and work between the RCMP and my office following these matters, but it does not relate to the current matter with the use of this new technology.

Mr. Parm Bains: The RCMP's response to the Order Paper question states that, in the past, the RCMP intercepted private communications and other data in motion pursuant to Criminal Code section 185 and subsection 186(6) authorizations, and other judicial orders and warrants. In your opinion, do these warrants provide sufficient protection?

Mr. Philippe Dufresne: Well, this is what we will want to answer once we have the specific information about the tools and their capacities. Certainly, it does provide protection and it does provide safeguards. Hopefully, it provides sufficient safeguards. This is what we'll be looking at when we have the briefing on the tools themselves at the end of August.

Mr. Parm Bains: What benefit does a PIA offer that a judicially approved warrant might not?

Mr. Philippe Dufresne: The judicially approved warrant will look at the specific request on the basis of the criteria in the Criminal Code and will follow that process. The PIA will look at it from a program perspective. It will look at it broadly in terms of what types of available tools are being used, what are the mechanisms to authorize the use of those tools, and whether the mechanisms are sufficient. For instance, should there be different or additional requirements before they can be judicially authorized, or should there be, in addition to the judicial authorization, mechanisms for the safeguarding of information? Perhaps that's not necessary, but the PIA serves that purpose—to look at it, not with respect to a specific case but with respect to the program as a whole.

● (1200)

Mr. Parm Bains: Do you believe that your office should be consulted on every use of ODIT, or should it be on a case-by-case basis?

Mr. Philippe Dufresne: With regard to being consulted on a PIA, I'm not suggesting that every time an ODIT is being sought in a given investigation we would be consulted—not at all. What I'm suggesting is that a PIA should be done on the program and on those tools, and that we be consulted with respect to this program and those tools generally, so that we can provide input as to whether the process as a whole is sufficient to protect privacy—not with respect to specific cases.

Mr. Parm Bains: How far along is the RCMP's privacy impact assessment?

Mr. Philippe Dufresne: I don't know. You would have to ask them that.

Mr. Parm Bains: Is there a timeline for when you expect to receive the PIA?

Mr. Philippe Dufresne: What I know is that we will receive a briefing at the end of August on these tools. I don't know if the PIA will be concluded at that time. That would be something to ask them, but I know that we will be receiving a briefing at the end of August.

Mr. Parm Bains: Do you have any concerns about the approval process for the use of ODITs? If so, how can they be addressed?

Mr. Philippe Dufresne: My concern is that the PIA in this instance was not brought to my office's attention before the tools were used. That's my focus—looking at how this program has been looked at from a privacy standpoint and having the ability to provide our input.

I don't have concerns that I can share right now in terms of the specifics because I have not seen the specific information.

The Chair: Thank you.

With that, we've completed two full rounds under the time portion that the committee's operating with. We're going to a third round now, beginning with Mr. Kurek for up to five minutes.

Mr. Damien Kurek: Thank you very much, Mr. Chair.

Some of the information has certainly been very revealing. There's one question that I'd like to ask to kind of dig into one of your previous responses.

The onus is upon government departments. I certainly know that scarcity of resources is a reality that your office faces, but the onus is upon government departments and agencies and, by extension, entities like the RCMP and whatnot to reach out to your office. However, the precedent that I see is certainly not very good. The fact is that the RCMP—I'm looking at the timeline—waited three years after starting to use this type of technology to do a privacy impact assessment and only reached out to your office after this went to the media a couple of years after that. That's not a good precedent.

We saw that the same sort of dynamic existed when it was dealing with the use of mobility data, facial recognition technology, and the list goes on and on. The fact that the onus is upon departments certainly doesn't give me much confidence that proactive work is being done.

I'd ask for your feedback, I guess, on my interpretation—certainly as a second-term parliamentarian now—that a lot of work has to be done to ensure that privacy is respected in our government.

Mr. Philippe Dufresne: Absolutely. This is something that I will be looking at in terms of what we, as the OPC, can do to help this process. The first position I'm stating is that the recommendation should be a legal obligation and it should be on the departments to do so, and to proactively do so.

I've been having good exchanges and meetings with my counterparts. It's been my first month as the Privacy Commissioner, and I've spent a lot of time reaching out and having good discussions. I sense a lot of goodwill, so I want to build on that and I want to create means of communication and exchanges, so I'll be looking to see how we can improve that.

● (1205)

Mr. Damien Kurek: Just to clarify that, by “counterparts”, do you mean provincial counterparts or those within agencies and departments? What do you mean by—

Mr. Philippe Dufresne: I mean both with respect to provincial counterparts and departments and with respect to the private sector. I'm going to continue that reach out to see how we can help that process to make sure the information flows.

Mr. Damien Kurek: I'm glad that the RCMP will be briefing you and your office come the end of August—although, again, it's disappointing that it's only under these circumstances that this is taking place.

I asked in my previous round for you to clarify if your office had safeguards in place to ensure the operational integrity of something like a law enforcement entity like the RCMP so that an investigation is not compromised, and whatnot.

I'd like to give you an opportunity to expand a little bit on that, especially as the RCMP and the Minister of Public Safety will be appearing before this committee a little bit later.

Can you expand on some of the steps that you and your office have to ensure that entities like the RCMP or other arms, agencies and departments of government can be assured that, if they reach out to you, the operational integrity of something like an investigation would be protected?

Mr. Philippe Dufresne: Certainly. We will put in place the mechanisms necessary so that if we receive information that is confidential, secret or top secret, obviously we want to protect that.

Again, that goes to the point that privacy is not an obstacle to the public interest. It's not in the public interest to jeopardize the confidentiality of investigative information, so looking at a privacy impact assessment has to be done in this context. If there's information that's of a particular sensitivity, then it has to be treated appropriately, and we would put the measures in place to do so.

Mr. Damien Kurek: Thank you very much.

It's the final minute or so of my questions, and you've talked about the updates that need to be made to the act. A minute is probably not enough time, but if I could, I'll ask you to provide to this committee the specific provisions within the legislation that need to be changed. There's an onus to have it codified, and not simply within the preamble of the legislation, so what specifically needs to be done? Certainly, as a committee member, I know it would be helpful for you to provide that information, probably in writing. That would be best, and if I could, I'll ask you and your office to do so in the coming days as we continue to look at this.

Mr. Philippe Dufresne: Absolutely.

Mr. Damien Kurek: Thank you very much.

Thank you, Mr. Chair.

The Chair: Thank you.

Next we have Ms. Hepfner for up to five minutes.

Ms. Lisa Hepfner: Thank you, Chair.

Mr. Dufresne, it sounds like you haven't seen the documents provided to this committee by the RCMP, so I'll share that in a letter from Commissioner Brenda Lucki, we learned that since 2017, the RCMP has used this ODIT technology—ODIT is the technology that they use to access people's devices—"in support of 32 investigations in which a combined total of 49 devices were targeted." This goes back to 2017. It's been used 32 times to access 49 devices. There's a list of the types of investigations the RCMP has used this technology for, and it's for things like terrorism, kidnapping, murder and trafficking.

It sounds like this technology has not been overused. What's your impression of the way the technology has been used thus far according to what we've learned from the RCMP?

Mr. Philippe Dufresne: This is exactly the type of information that needs to be looked at in a PIA, with my office being consulted on it. This is the type of thing that would certainly go towards saying, okay, there are mechanisms here for approvals, so is it being used in specific, tailored cases appropriate to the severity of what's at stake and so on and so forth? These are the types of things.... It is very relevant information to consider and is part of what we look at in terms of necessity and proportionality, absolutely.

Ms. Lisa Hepfner: Would you say that there are circumstances in which the RCMP should be allowed to use this technology? I ask because it's not useful to tap a home phone as people aren't using those anymore, and people who may be committing terrorism, murder or kidnapping shouldn't have the right to privacy; they should lose that right.

Can you talk about whether this is useful technology in some cases and whether some people shouldn't have the right to privacy?

● (1210)

Mr. Philippe Dufresne: Well, I think what's important is that the tools are looked at in terms of their impact, their purpose and the importance of the public interest at play. It's not a zero-sum game, and it's that not you achieve the public interest by sacrificing privacy. You achieve both. However, there certainly is an argument to be made to have some requirements for authorization in the Criminal Code, approved by Parliament, that provide some specific conditions and information about the types of situations where it can be used.

These are all things we would be looking at to see if there's more we could recommend to make this stronger from a privacy standpoint. Maybe there will be; maybe there won't be, but the important thing is that this exercise takes place, because it could strengthen the program. Maybe we won't need to strengthen it because the program is already strong enough, but this will strengthen trust because it will reassure Canadians that there's been a vetting of this from a privacy standpoint.

Ms. Lisa Hepfner: Thank you.

Can you talk about some of the checks and balances that are already in place? For example, we learned that the RCMP needs two types of warrants to use this technology: a transmission data recorder warrant and a general warrant. They have to be approved by a judge and have to go through a special department of the RCMP. Can you talk about that a bit further?

Mr. Philippe Dufresne: I think this is something the RCMP will be very well placed to talk about in terms of the details, but I can say that there is a requirement for judicial authorization and there are criteria for obtaining this judicial authorization. There are some specific time periods for the duration. There are also requirements to notify the individuals at the end of the process and there's the possibility for extending that. There are a number of safeguards that exist, so the question will be whether there are other things that could be required or recommended given the privacy intrusiveness. As I said, maybe there will be; maybe there won't be, but going through that exercise will be important.

The Chair: You had maybe a few seconds left , Ms. Hepfner. I'm not sure; maybe you were muted or you had a—

Ms. Lisa Hepfner: I was muted. I'm sorry. I was just signing off anyway because I realized I only had a few seconds left.

Thanks very much, Chair.

The Chair: Now we're at five minutes.

With that, we'll go to Mr. Villemure for two and a half minutes.

Go ahead.

[*Translation*]

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

We are discussing the right to privacy as a fundamental right, one that is in the public interest and promotes a sense of trust. Those things are undermined, however, when media reports reveal that organizations are using these tools.

Do you think we need a public debate on privacy and the use of these technologies?

Right now, people are worried and they don't understand everything that's going on, because it's complicated. Is a public debate warranted?

Mr. Philippe Dufresne: I would say a public debate is under way as we speak given what this committee is studying. You are playing an important role by asking these questions and studying the issue. Your recommendations will fuel that debate.

Raising privacy concerns and discussing the interplay with new and evolving technologies is important, so that Canadians are aware of what's going on. It helps inform them about new technologies and the safeguards in place to protect their privacy.

When Canadians find out that a parliamentary committee like this has the ability to examine the privacy repercussions of these tools, to consult my office and to make recommendations, it helps earn their trust. It shows them that there is a regime in place, that Canadians aren't on their own when it comes to defending their privacy.

Mr. René Villemure: Do you think it's necessary to educate people about privacy issues?

Mr. Philippe Dufresne: One of the things I said earlier is that more needs to be done. Young people need to be educated, whether at the high school, CEGEP or university level. We live in an increasingly digital world, so these are issues we need to talk about more with young people.

● (1215)

Mr. René Villemure: Thank you very much.

[*English*]

The Chair: You have 30 seconds.

[*Translation*]

Mr. René Villemure: Commissioner, my fellow member asked you to get back to the committee with some written information, but I'm curious as to whether you have the technical expertise to assess these new technologies.

Mr. Philippe Dufresne: Yes, we have a very strong technical team. Assessing technologies is part of what we do. We make sure we keep up with the latest technologies and have cutting-edge expertise.

Mr. René Villemure: Thank you very much.

[*English*]

The Chair: Thank you.

We have Mr. Green now for two and a half minutes.

Mr. Matthew Green: I'd like to continue on that line.

I'm sure that you've been looking at budgetary concerns since you've come into your new role. Do you believe that your department is set up contemplating a proactive approach to the assessments and the rapid advance of technology? Do you believe that you're set up and fully funded in a way that you'll have all the tools and resources necessary to keep up with the subject matter expertise and this growing explosion of surveillance tools that are being used?

Mr. Philippe Dufresne: We're certainly looking at the resources situation very carefully. We have had the Privacy Act extension order that extended the ambit of the Privacy Act. We've made a request for more resources based on that. We're waiting for the answer to that request.

We're also looking at Bill C-27. We're looking at potential modernization of the Privacy Act itself. All of these are raising questions of resources. Not everything requires more resources, but I'm certainly looking at this very carefully as one of my focuses to see if we have what we need and what we will need so that we can be as efficient as we need to be to face these new challenges and realities.

Mr. Matthew Green: Thank you.

Mr. Chair, even going through some of the preliminary supporting documents, one of my concerns, as somebody who likes to think they're somewhat technologically savvy, remains that there's just so much out there that we know we know and we know we don't know, but then we don't know what we don't know. My concern is that we have a generation of court justices, of judges, who are making decisions on proportionality who may not have, quite frankly, the technical expertise to keep up with making adequate decisions on exactly what it is they're giving warrants to.

In the contemplation of the Privacy Act, are there specific legal frameworks that you would like to see that might help guide our judiciary to make the adequate assessments on whether this is proportionate?

Mr. Philippe Dufresne: We need to make sure, whoever the decision-maker is, whether it's the judiciary, my office or departments, that they have the necessary understanding of the technology that's at play. We need to understand the privacy impacts. We need to understand the information at play, and we need to understand what the capabilities are and if those change the nature of the discussion of metadata.

We have privacy legislation in the public sector that's 40 years old. We have the private sector. We have Bill C-27 that's going to be considered to modernize the private sector, so it's important that the legislation keeps up, but also, as you rightly point out, that the decision-makers are properly equipped with that knowledge. In this case, it's technological knowledge.

The Chair: Thank you.

Now we'll go to Mr. Williams for five minutes.

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

Following the vein of not knowing what we know don't know, certainly when we're looking at this kind of technology and what we've just learned, this was started in 2018. Knowing how technology evolves, we probably have a lot more technology that could be used that we have no knowledge of.

I want to go into some of the recommendations that you may or may not make from your end for our report on this issue that we're studying right now. I know that you're going to submit some of these in writing. Specifically knowing what this specific software can do perhaps from your research, is there anything new you would recommend for the Privacy Act that we didn't have before on facial recognition technology or on mobile data?

Mr. Philippe Dufresne: I will wait to get the briefing on those specific tools to see all of the capabilities they have, but I think that we need to make sure that the legislation, when it's amended, is done in a way that it can keep up with technology. We can't amend legislation as quickly as technology evolves, so how do we make sure that the legislation is flexible enough to keep up with this technology that's going to be evolving? I think the questions remain the same, namely focusing on the impact, on the privacy intrusive nature of these tools and comparing that to the goals and making sure that it goes no further than what is required by the goal.

● (1220)

Mr. Ryan Williams: Based on some of my research, there are a tremendous number of loopholes that technology exploits to be able to use that. One of those is that, if satellites cross earth's orbit and information is contained in that satellite, there are ways it can be stored in other countries. Canada can get that through other ways, but we have specific loopholes that we just haven't caught up with, and we're finding that out here. Is that something else your office is investigating and looking into when it comes to being as modern as possible when we redo these privacy laws?

Mr. Philippe Dufresne: We're working very closely with our international counterparts and seeing how we can work together, put forward similar principles and deal with these issues that, in many regards, know no borders. That's part of what we do in our international outreach and sharing of information.

Mr. Ryan Williams: In terms of the public versus private sectors, I know this has come up before. There are sometimes different rules for the private and public sectors.

You've also talked about working with the provinces. Specifically when it comes to privately and publicly working with the provinces, are we developing best practices in order to look at this technology as a whole federally and provincially?

Mr. Philippe Dufresne: We have great working collaborations with the provincial counterparts. This is my first month, but I was told that there are monthly calls and regular discussions and exchanges. We do keep a close relationship to work with each other and to make sure that our respective legislation evolves in the right way. We learn from best practices in one area. My goal as the federal Privacy Commissioner is making sure I can give the best advice and recommendation to Parliament so that the federal legislation is as good as it can be.

Mr. Ryan Williams: Similarly, looking across the world at our European partners, is your office in contact with them, too, looking at what their privacy laws look like privately and publicly?

Mr. Philippe Dufresne: Absolutely. We have very close collaboration. I have already had exchanges with my counterparts since the start of my term on June 27. We're looking at the GDPR. We're looking at developments in the U.S. and developments in the U.K. We're facing similar challenges, and there are different approaches that are adopted. My office's goal is to look at what will work best for Canadians and to provide recommendations to Parliament via this committee.

Mr. Ryan Williams: To echo my counterpart, does your office at this point need any more resources to find more of that collaboration?

Mr. Philippe Dufresne: At this point my office does need more resources. We've made a request for more resources already and we're awaiting the response on that. We are evaluating what we will need for Bill C-27 and beyond.

Mr. Ryan Williams: Thank you very much.

Thanks, Mr. Chair.

The Chair: All right. With that, we'll go to Ms. Khalid, who will be last in this third round.

Go ahead, Ms. Khalid.

Ms. Iqra Khalid: Thanks, Mr. Chair.

I know we've been talking a lot about the need for transparency to build trust in public institutions, but on the flip side of that, do you think, for example, that somebody watching this committee hearing is going to come away with the takeaway that the RCMP is doing mass surveillance on them? Are we finding the right balance and holding institutions to account? Is there a responsibility on us to also reassure the public that mass surveillance is not happening, if that's the case? What's your role in that regard?

Mr. Philippe Dufresne: I think that's an important point. When I talk about privacy as an accelerator of the trust Canadians have in their institutions, I mean that. It's important that Canadians are reassured about the processes that exist and about their institutions and what their institutions are doing.

In this case, I think Canadians will see that the RCMP is providing responses to Parliament, will be appearing and will be sharing information and answering questions by this committee. They will be playing a fundamental role in obtaining information and providing advice to the House in its report. I think this is a strong functioning system.

What I am advocating for is to see even more of that in the context of privacy impact assessments at the front end. I think that would even further generate some of this trust and would perhaps allay concerns that may arise—perhaps needlessly—when something becomes public in the media and creates some doubts. At the end of the day, they may be unwarranted, whereas if this had been looked at earlier on, perhaps there would have been a way of allaying doubts even earlier.

● (1225)

Ms. Iqra Khalid: To continue with that, I know some of my colleagues across the way said the RCMP is conducting mass surveillance on the population and on MPs. Do you have any comments on that? Is there any evidence of that?

Mr. Philippe Dufresne: I know that my officials have good working relations with the RCMP, and I look forward to having the same with Commissioner Lucki and the institution. What I am saying is there's a good opportunity to conduct a PIA to provide information. We're available to work with the RCMP to provide advice on these tools.

Ms. Iqra Khalid: Thanks for that.

Do you have any concerns about the public disclosure of policing techniques and technologies? How do we balance the public's right to know with the risk of criminal organizations getting ahead of our investigative tools?

Mr. Philippe Dufresne: This goes to when I talk about privacy not being an obstacle to the public interest but building on each other. That's very important.

There may well be information that cannot and should not be made public. If we're talking about criminal investigative techniques, there's probably a good potential that that would apply in this instance. Doing a PIA internally, consulting my office confidentially and putting in place necessary safeguards would not go against that. We'd look at it on a case-by-case basis, but not everything can be made public. That's something that would be looked at on the facts of a case.

Ms. Iqra Khalid: Based on that, do I understand you correctly that you're seeking to find a balance between privacy rights and working competently to protect the safety and security of Canadians through the PIA system? In other words, are you arguing that legislated PIAs will help governments, agencies and individuals find a balance between privacy and security?

Mr. Philippe Dufresne: I think that's a very good way of formulating it. I would agree with that. Privacy is a fundamental right. It needs to support the public interest. One of the ways of doing that, while generating trust, is to have PIAs at the front end and a good process for reviewing them.

Ms. Iqra Khalid: Thank you.

Last, I'll just ask if there's anything that you'd like to add to what you've been asked today as words of advice for our committee or a recommendation that you want to put forward before us.

Mr. Philippe Dufresne: I think that there have been lots of good questions and exchanges, and I don't have anything to add top of mind, but we will be following up with the committee with the specific wording of our recommendation for the legislation.

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

Thank you, Chair. Those are all my questions.

Mr. Matthew Green: Excuse me, Mr. Chair.

The Chair: Thank you.

Go ahead, Mr. Green.

Mr. Matthew Green: Mr. Chair, I'd just like to request that, with the time remaining, the committee go back to its practice in first round in terms of the order and time allocations.

The Chair: At the end of this round, I was going to canvass the room to see if there was interest in continuing and having additional speakers. I can see there is such an interest. I thought that, after concluding three full rounds, I'd check first, but we do have the commissioner for another half hour, so maybe just give me a quick show of hands to see who would be interested in another speaking round.

I think what I will do is proceed as Mr. Green has suggested. I'll take four more speakers, and I'm going to cut it to five minutes each. Let's just do five each.

I see Mr. Bezan, Mr. Villemure and Mr. Green. I haven't seen any hands up yet on screen. Now I see one. All right, Ms. Khalid, I'll have you up, and I'll maybe just go in the regular order and have Mr. Bezan go first for five followed by Ms. Khalid, Monsieur Villemure and Mr. Green.

Go ahead, Mr. Bezan.

● (1230)

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

Going back to Commissioner Dufresne, I am concerned that there hasn't been complete transparency here, never mind concerns around the issue of privacy. When you look at the track record of this committee's work, we've started down the mobility data avenue, and the Public Health Agency of Canada and the Minister of Health never went directly to the Office of the Privacy Commissioner to get advice. There was some information sharing, but there was never an ask for input from the Privacy Commissioner's office.

When we studied facial recognition technology, it was after the fact that we learned about Clearview and how they're using artificial intelligence, and the shortfalls in monitoring, and it was only after it became public that police agencies in Canada decided to quit using FRT from Clearview, in particular, and now we are here talking about ODIT and software companies like NSO that has the Pegasus spyware. You have all of these, as they've been described: mercenary data companies that are out there selling this not just to police agencies but also to other governments with access worldwide.

Are you not concerned that, as the RCMP, CSIS and other government agencies are using this commercially available technology, it could fall into the wrong hands, never mind the privacy breaches that can occur with the use of that technology here in Canada?

Mr. Philippe Dufresne: I think privacy breaches are always something that we have to be guarding against, and my office should be informed of them when they occur, and the more sensitive the information an organization holds, the stronger the protection should be in terms of those breaches. That's fundamentally important.

I think the potentially highly intrusive nature of these tools warrants that they be looked at from a privacy standpoint. Whatever the tool is, it needs to be looked at from its impact and needs to be looked at in terms of proportionality and minimal use, and, if there's a risk of private sector use, well, that has to be looked at within that context of private sector use, which is going to have far different justifications from the public sector in terms of law enforcement.

Mr. James Bezan: As we look at the use of ODIT and look at the Pegasus software system in particular, the U.S. found that it was being used by malign actors and other foreign state actors within the United States. Do you have concerns of that potentially happening here as well?

The U.S. Congress has banned the use of Pegasus in the United States.

Mr. Philippe Dufresne: From what I see in the reports about the use of software like Pegasus directed at citizens without authorization, these are concerning allegations. This is something that, if it occurred in Canada, would certainly raise concerns.

Mr. James Bezan: Again, this comes down to trust in our institutions—between Canadians and the RCMP, Canadians and Parliament, Canadians and government agencies. When we had this question on the Order Paper returned, the RCMP said they'd used ODIT 10 times. Now, as referred to by one of the Liberal members, we have a letter from Commissioner Brenda Lucki to our committee. They're now saying that it's been used 32 times, yet they refuse to follow this committee's request for information on the details of the warrants that were used. The warrants are under all different aspects of the Criminal Code and our charter rights, so we have to be concerned about how it's being used that way.

Also, the RCMP refuses to disclose whether they are using this type of spyware here on the Hill, against parliamentarians, against our staff or against departmental officials.

How do you feel about the RCMP...? Again, the yardsticks keep moving. They refuse to comply with Parliament's supremacy here in getting information and are withholding critical information that this committee has requested, which would also help inform your office on how ODIT is being used in Canada.

● (1235)

Mr. Philippe Dufresne: I think these are questions that could be asked of the RCMP members. My focus is with respect to my office's role being consulted on the privacy impact assessment. I look forward to seeing that at the end of August. I would have liked my office to have seen that already, but, looking forward, we will review it, and we'll provide our best advice to ensure that this properly takes into consideration the privacy of Canadians.

Mr. James Bezan: Thank you.

The Chair: Thank you.

Now we have Ms. Khalid for five minutes.

Ms. Iqra Khalid: Thank you, Chair.

On the line of questioning by Mr. Bezan, I've heard multiple times now from that members opposite that there's a lack of transparency in this whole process with the RCMP and on who's being surveilled. There are suggestions being made that MPs are being surveilled, that the general public is being surveilled.

I know you said this before, Mr. Dufresne, but I'll ask you again. Do you have any evidence or indication that this is the case?

Mr. Philippe Dufresne: I don't have any evidence that this is the case. I look forward to receiving the information on the use of those tools at the end of August.

Ms. Iqra Khalid: Do you think that it would be right for you or your office to review the work of a judge signing off on a warrant for an investigation by the RCMP?

Mr. Philippe Dufresne: No. What I'm talking about with privacy impact assessments is really looking at the program as a whole at a macro level—not looking at an individual decision made in an individual case. Rather, it would be looking at the process. What are the criteria? What are the safeguards that could be put in place?

Ms. Iqra Khalid: Thank you.

I think my colleague also spoke about private organizations and the way they are selling technology. For example, the Awz group is selling technologies sold by our former Prime Minister Stephen Harper. Should he be allowed to sell that technology, which is so invasive, so intrusive? Should there be limits on who he should be able to sell it to?

Mr. Philippe Dufresne: There is private sector privacy legislation, which raises these types of issues in terms of collection and use by private organizations. Again, the specific privacy-intrusive tools are going to be looked at differently, whether they're used for purely commercial purposes or for a public interest purpose by law enforcement authorities.

Ms. Iqra Khalid: Thank you.

Mr. Chair, do I have time left?

The Chair: Yes, you have at least a couple of more minutes. You have close to three minutes.

Ms. Iqra Khalid: Thank you.

Mr. Dufresne, I know that we've talked about this before with respect to the PIAs striking that right balance. In your opinion, are there any missing pieces or gaps within how that PIA would strike that right balance that we are trying to achieve to increase transparency and accountability of government?

Mr. Philippe Dufresne: I think the PIA process, the way that it's described in the Treasury Board policy and the way it is described in the advice by my office on what we look for in PIAs, is very comprehensive. It balances risk. It looks at situations in their proper context, and it puts the efforts where they need to be put, and it is something that can achieve public interest goals while protecting fundamental privacy rights. I think this is a good tool. It's a flexible tool. It's not something that should be seen as a check or a nuisance. It's something that really helps the decision-making process and makes the program stronger from all aspects. I do highly commend it, and I think it should be something that is done as soon as possible. Mind you, there will be situations where exigent circumstances will prevent that from happening, but the standing point should be, as much as possible, to do that before the program is launched.

Ms. Iqra Khalid: Are these conversations that you're having with your provincial and territorial counterparts as well with respect to provincial law enforcement?

● (1240)

Mr. Philippe Dufresne: We are talking about all issues relating to privacy. We're talking about trends, and we're looking at what to expect in terms of law reform and evolving technology. We haven't spoken about this specific topic.

Ms. Iqra Khalid: Thank you.

Those are all of the questions I have, Chair.

The Chair: Thank you.

Go ahead, Mr. Villemure.

[*Translation*]

You have the floor for five minutes.

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

Mr. Dufresne, I'm going to ask you the same question my fellow member—

[*English*]

Ms. Iqra Khalid: Excuse me, Mr. Chair—

The Chair: Yes.

Ms. Iqra Khalid: I'm very sorry. If it's okay, I just want to clarify with respect to our routine motions on subsequent rounds, whether we are doing five minutes per member. I ask because I know that our routine motions listed times that are a little bit different. I just need some clarification.

The Chair: Yes, I am deviating from that. That was what I had said. I was canvassing the room if we wanted to end the meeting after the third round, and then I asked who maybe wanted to speak. There were a number of people who did. I made a ruling to let each party have a five-minute round. That was my ruling, and I'm going to give Mr. Villemure five minutes and Mr. Green five minutes, and I might have a question from the chair when we're done.

[*Translation*]

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

I'm going to ask you the same question my fellow member asked you.

Commissioner and Deputy Commissioner, do you think spyware was used to surveil Canadians in general?

I'm not asking for documented evidence. I'm simply asking whether you think it's happened.

Mr. Philippe Dufresne: We know that spyware was used because the RCMP confirmed it. What we want to see is the privacy impact assessment for the program.

Mr. René Villemure: Can you comment on that, Mr. Smolynec?

Dr. Gregory Smolynec: Whether that happened, I'm not aware.

Mr. René Villemure: All right.

I was talking about what goes on beyond government. In general, do you think spyware is being used to surveil Canadians?

Mr. Philippe Dufresne: I will repeat what I said about the information we received about what took place. Other witnesses will be able to share their experiences.

Mr. René Villemure: Very well.

When you carry out a PIA and you identify gaps—say, in one of Apple's or Samsung's systems—do you flag them to the phone manufacturers, to ensure users' privacy is protected?

Mr. Philippe Dufresne: Mr. Smolynec may be able to say more about that.

I do think we would share our findings with them to ensure that privacy is protected.

Mr. René Villemure: That means your staff would be in contact with the phone manufacturers to ensure that harmful gaps were plugged.

Is that right?

Mr. Philippe Dufresne: We have consultation mechanisms for the government and for the business community. Organizations are able to reach out to us about potential initiatives. We conduct assessments on a case-by-case basis, so we can provide feedback and advice on privacy considerations.

Mr. René Villemure: If you identify a gap, do you proactively contact manufacturers like Apple to ensure the gap is plugged?

Mr. Philippe Dufresne: If we identify a gap and we weren't contacted, it is possible to file a complaint in some cases or to proactively initiate discussions with the organization in others.

Mr. Smolynec may have more to say on that.

Dr. Gregory Smolynec: That is a possibility.

Mr. René Villemure: I see.

You wouldn't do nothing, then.

Isn't that right?

Mr. Philippe Dufresne: No, we wouldn't do nothing.

Mr. René Villemure: Thank you very much.

This year, Canada is chairing the Freedom Online Coalition, which promotes best practices.

Do you think it would be appropriate to examine the use of spyware?

Would it be a good idea for Canada to propose that to other countries so that, together, we can come up with best practices?

Mr. Philippe Dufresne: This issue has captured the public's attention, especially thanks to this study. The issue is under the media spotlight. Canadians are concerned about anything having to do with their digital tools.

Mr. René Villemure: The issue is on people's radar thanks to articles that appeared in La Presse and on news site Politico. Did you become concerned when you read those reports?

All of this is quite shocking when you consider your earlier point about the public interest, privacy as a fundamental right and Canadians' trust.

If you put yourself in the average person's shoes, does the information in those articles worry you?

● (1245)

Mr. Philippe Dufresne: A stronger regime is needed when it comes to the requirement to prepare PIAs. That is the basis for my recommendation. After reading the articles, I realize how important it is to be able to tell Canadians that privacy impact assessments are being carried out and that privacy authorities will be consulted. I think that would reassure Canadians.

Mr. René Villemure: I want to follow up on something we talked about earlier.

We all know that technology moves faster than legislation, which tends to play catch-up, so do you think a moratorium on the use of these tools is warranted?

Mr. Philippe Dufresne: I'm going to wait until I've seen the presentation on the tools in question before I give an opinion on that.

Mr. René Villemure: Are you referring to the presentation you'll be getting from the RCMP in August or another presentation?

Mr. Philippe Dufresne: I'm referring to the RCMP's presentation in August. That's when I'll get the information on these tools.

Mr. René Villemure: The presentation will be on the RCMP's use of the tools.

Is that right?

Mr. Philippe Dufresne: Yes, that's right.

Mr. René Villemure: Other organizations, government or otherwise, may be using the tools. We don't know, but we do know that surveillance is a $12-billion industry. I think we need to be proactive in seeking that information. There are four or five Israeli tools, alone. Pegasus is one, but there are others.

Will you work proactively to find out whether organizations other than the RCMP are using these tools?

Mr. Philippe Dufresne: I think it's appropriate to see how the use of these tools by police forces like the RCMP compares with their use by the private sector. That gives rise to other questions.

Mr. René Villemure: Will you be addressing the issue from a private sector standpoint, or do you wait until a complaint comes in?

Mr. Philippe Dufresne: We are going to examine the issue internally to determine whether we are going to make recommendations or take steps to address the issue in the private sector.

Mr. René Villemure: I see.

When would you like to see new legislation containing your recommendations adopted?

Mr. Philippe Dufresne: My recommendations on—

[*English*]

The Chair: Thank you.

We'll go to Mr. Green for the final five minutes.

Go ahead.

Mr. Matthew Green: Thank you.

Mr. Dufresne, are you aware of the use of stingray technology, the dummy cellphone towers that are set up to capture information as it comes and goes?

Mr. Philippe Dufresne: We had an investigation on cell site simulators. We looked at the RCMP's use of those tools.

Mr. Matthew Green: What did you find in that investigation?

Mr. Philippe Dufresne: In that investigation, we found that when it was authorized by a judicial warrant, it was compliant with privacy legislation. There were instances where we had not received sufficient evidence to indicate that it was judicially authorized or that there were exigent circumstances.

Mr. Matthew Green: Just to be clear, you're stating here on the record that the RCMP was using—I think it's commonly called stingray technology—artificial cellphone towers to intercept information without warrants.

Mr. Philippe Dufresne: We said in our investigation that, in certain instances, they did not have warrants. I believe their position was that these were exigent circumstances, and we didn't have information from them on that.

Mr. Matthew Green: When this technology is used, do you understand it to be true that it captures everybody's information and doesn't necessarily have the ability to target individual phones?

Mr. Philippe Dufresne: I'm not sure if Dr. Smolynec can answer this one more specifically.

Dr. Gregory Smolynec: No, I can't answer more specifically.

Mr. Matthew Green: I think this is another example of where we see the RCMP using technology in a way that may or may not have judicial review.

In your opinion, what concerns do you have regarding the use of technologies like the one we're considering both on device and other ones? Stingray technology is just one step away from that in gathering the information outside of the device. What concerns do you have about that? How does the use of this technology by law enforcement affect the fundamental right to privacy that you laid out in your opening remarks?

Mr. Philippe Dufresne: I think what it shows is that judicial authorization is very important when law enforcement authorities are using these types of tools to intercept private communication and personal information, so that's essential. In that investigation, we found that, in certain circumstances where there was no such authorization, we wanted to see information about exigent circumstances, so that is something we look at—

Mr. Matthew Green: Could I pause for a second, Mr. Chair, on that point? Given your history and your understanding of the charter and breaches of the charter, what happens when law enforcement uses this technology without judicial oversight? What are the ramifications? What are the outcomes and consequences of that use?

● (1250)

Mr. Philippe Dufresne: It's important that there be oversight of the use of those tools. Those tools are intrusive. They have access to the private information of Canadians, so that's why Parliament has put in place judicial authorization regimes. That's why we have the charter, all of these limits, for the fundamental rights of Canadians. In the context of privacy, the question we're asking today is: In circumstances where there is judicial authorization and where there is a regime, do we need more in terms of privacy consideration given the power—

Mr. Matthew Green: My apologies; that's not the question I'm asking today. The question that I'm asking is what happens in a culture.... You've referenced a culture of privacy. I'm suggesting to you that there's a culture of cavalier intrusions on privacy and shortcuts that are taken. We had Clearview before us for a study of ours, where a lower-level police officer suggested that somebody just took it out on a whim. We had an RCMP officer refuse to name the person who authorized it, in what I believe to be contempt of this committee.

The question that I'm asking isn't so much in the perfect scenario, but what are the threats and risks involved in situations when an officer goes rogue, for whatever reason, or doesn't necessarily have the oversight, even within the RCMP, quite frankly, to do the things that they're doing, given the expansion of technology and the industry's propensity to offer this stuff even through, as I'm hearing anecdotally, on a trial basis and for free to kind of circumvent procurement?

Mr. Philippe Dufresne: What I think it shows is that in Canada Parliament has taken steps to put in safeguards on the use of this information. It's important that these safeguards exist because of the impact that this technology, these tools, can have on citizens and on fundamental rights.

Mr. Matthew Green: Mr. Chair, through you, respectfully, do they exist? Because if they existed, we wouldn't necessarily be here right now, would we?

Mr. Philippe Dufresne: In this instance, what I'm saying is that there is a process to do a privacy impact assessment on the use of new tools.

Mr. Matthew Green: I respect that, and I respect your newness to your position. I would put to this committee that, in fact, the guardrails don't exist, which is why we're here in the summer examining something that was really only discovered due to the diligence of the media.

Thank you.

The Chair: Thank you, Mr. Green.

Before we wrap up, I have a couple of points.

I don't ask a lot of questions from the chair, but I'm going to take a minute or two here.

Commissioner Dufresne, in a response to one of your questions earlier, you talked about the committee's ability to deal with sensitive information. You are a former law clerk, and you're probably uniquely qualified to give us a little more detail on how that works for the benefit of committee members.

I'll let you go ahead with that.

Mr. Philippe Dufresne: I'll answer that not wearing my law clerk's hat and just talk about the constitutional law principles and the committee's authority to send for papers and records and to act as the grand inquest of the nation. You have the ability to seek information, to sit in camera and to put in place mechanisms to protect the confidentiality of information that you request for your studies.

The Chair: Thank you.

In their response to the Order Paper question that really caused this study, the response, the public reaction and the committee's decision, the RCMP said that the unit worked closely with the Public Prosecution Service and the Privacy Commissioner. Your testimony this morning did not seem to indicate that. Is that correct?

Mr. Philippe Dufresne: I think that is referencing a different unit of the RCMP, not the program that is using the ODIT. I think that's the distinction—

The Chair: Which program is it? Just so that we're clear, if you're able to differentiate between the two programs, that might help the committee.

Mr. Philippe Dufresne: My colleague can correct me, but I think they were talking about the Special “I” program, in place since 1975, as opposed to the CAIT program, which was—

● (1255)

The Chair: Okay. Thank you for clarifying that.

With that, I think we're just about out of time. I don't really want to get into final—

Mr. James Bezan: There's some clarification I need from you, Mr. Chair.

The Chair: Go ahead, if it's a point of order.

Mr. James Bezan: Mr. Chair, there have been some discussions about some of the documents the committee has received from the RCMP, particularly correspondence from Commissioner Lucki. Because they have been discussed at this committee, can we make public the documents that have been provided by the RCMP to the committee?

The Chair: Some of them have already been made public in the course of this meeting. Some committee members made reference to them. I'll have a brief moment with the clerk to ensure that I understand correctly that yes, they can be referred.

Any document that is supplied can be made public unless the committee agrees otherwise. Any of the material that the committee received can be made public.

The clerk is looking for my attention. One moment.

The material that's supplied is not private to the extent that it can't be referred to in committee, but at the same time, if it were to be made public via the committee's website, for example, the committee would have to agree to it. The material is not secret. Members did, in the course of this meeting, refer to it and read portions of it into the record, so it can be made public. It's a matter of the will of the committee. You can choose to ask the clerk to place the material on the committee's website, for example.

Mr. James Bezan: Mr. Chair, I move that the material provided by the RCMP for the study on-device investigation tools used by the RCMP be published on the committee's website.

The Chair: Your motion is in order. I consider this the correct way to ensure that if the committee desires to have the material we've received made public, we do so.

For discussion, I see Mr. Fergus and Ms. Khalid. I'm going to go to Ms. Khalid.

Go ahead.

Ms. Iqra Khalid: Thanks, Chair.

I'm trying to seek some clarity as to why. What is the purpose of putting these documents to the public? I'm wondering if there is anywhere we are going with this. Clearly we'll be hearing from the RCMP this afternoon. It would perhaps be more efficient to do this after the RCMP has been here so that we can pose these questions to them as well.

I'm not sure why we're having this conversation in the last two minutes of the meeting, but I'm seeking some clarity as to what the objective of this is.

The Chair: I'm not in a position to answer that question, so I'll carry on. I've got Mr. Fergus next, and I see Mr. Kurek with his hand up.

Go ahead, Mr. Fergus.

Hon. Greg Fergus (Hull—Aylmer, Lib.): Thank you very much, Mr. Chair.

Could I ask if the chair could allow us to have five minutes to discuss this motion because these materials were requested. I would just like to know a little bit more about what the implications are. I would just like to have a couple of minutes to consider Mr. Bezan's motion.

The Chair: At a minimum, I think I would like to excuse our witnesses. We've completed our questions of our witnesses so, with our thanks, we'll allow them to leave if they would like to.

In terms of managing our time, if we have the committee resources to extend this meeting a few minutes, because we're at the hour, I'd be inclined to proceed as Mr. Fergus has suggested and return to this in a few minutes.

● (1300)

Ms. Iqra Khalid: Mr. Chair, I have other obligations at 1 p.m. that I need to get to. It's kind of going back on the whole principle of no surprises. I leave it to you, Chair.

The Chair: I have Mr. Fergus who wants a few minutes to confer with colleagues. I don't want to extend this meeting past—

Mr. Damien Kurek: I'll take my name off the list.

The Chair: Okay, at this point I have no further speakers.

I have a request for—

Hon. Greg Fergus: I'm sorry, Mr. Chair.

The Chair: Go ahead, Mr. Fergus.

Hon. Greg Fergus: If it's inconvenient for members to continue or if it's impossible for us to extend beyond one o'clock, perhaps we could save this discussion for the next meeting.

The Chair: Right now, I have no further discussion in front of me, unless others wish to speak to it.

We don't have time later in the day. The afternoon panel is compact, and I'd rather not have this spill over too much. If there are concerns about a decision to make public what has been turned over to the committee that is not private and that any member can access and read into the record, we're simply....

Well, I don't want to speak to the motion, but I'd rather put this to a vote and dispose of it, if there are no other speakers. If there are other people who wish to speak to it....

Go ahead, Ms. Khalid.

Ms. Iqra Khalid: Chair, I move to adjourn this meeting.

The Chair: We have a motion to adjourn this meeting, which is not debatable, so we'll put that to a vote immediately.

It's a tie. Accordingly, the Chair will be voting against the motion.

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

The Chair:

We are back to the motion of Mr. Bezan to make public that which the committee has received. Again, just to clarify this: these are public documents. The question before us is merely whether to publish them. They are public. The question before us is whether we make it easier for people to find them or not.

Ms. Khalid, go ahead.

Ms. Iqra Khalid: Thanks, Chair.

I just want to clarify this. It's not that I'm opposed to disclosing documents or making them more accessible to the public. It's the no-surprise-us thing. You know, we're willing to work with the whole team here, and at the 11th hour we're getting motions coming up.

Members have our contact information. I would like to work in a more collaborative fashion as opposed to a more hostile or oppositional one.

Chair, I just want to put that out there for members who are willing to work with us and work on these important issues. Let's work together a little bit more, folks.

The Chair: That's noted.

Is there any other discussion?

I will call the question. In the hybrid format, I will ask this in reverse. Is there anybody opposed to the motion?

Some hon. members: No.

The Chair: I see no opposition to the motion, so the motion is carried.

(Motion agreed to [*See Minutes of Proceedings*])

The Chair: With that, this meeting adjourned, and we will be back this afternoon.