HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

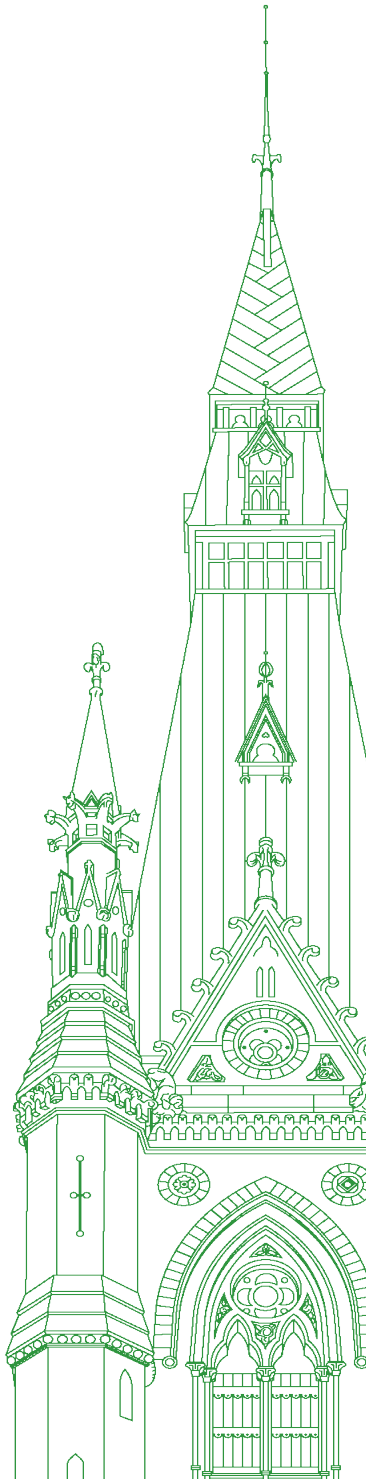
44th PARLIAMENT, 1st SESSION

Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 101

Tuesday, February 6, 2024



Chair: Mr. John Brassard

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, February 6, 2024

● (1100)

[*English*]

The Chair (Mr. John Brassard (Barrie—Innisfil, CPC)): Good morning, everyone.

I'm going to call the meeting to order.

[*Translation*]

Welcome to meeting number 101 of the House of Commons Standing Committee on Access to Information, Privacy and Ethics.

Pursuant to Standing Order 108(3)(h) and the motion adopted by the committee on Wednesday, December 6, 2023, the committee is resuming today its study of the federal government's use of technological tools capable of extracting personal data from mobile devices and computers.

Today's meeting is taking place in a hybrid format, pursuant to the Standing Orders. Members are attending in person in the room and remotely using the Zoom application.

[*English*]

I just want to remind everyone—I know the witnesses are aware of this—that the earpieces are not to be close to the microphones because that does cause feedback for our interpreters and potential injury as well.

I'd like to welcome our witnesses for the first hour this morning.

From the Department of Natural Resources, we have Francis Brisson, assistant deputy minister and chief financial officer, and Pierre Pelletier, chief information officer. From the Department of National Defence, we have Dave Yarker, director general, cyber and command and control information systems operations, and Sophie Martel, acting chief information officer.

We have five minutes for the opening statements.

I assume, Mr. Yarker, that we're going to go with you, sir, or is it Ms. Martel?

Ms. Sophie Martel (Acting Chief Information Officer, Department of National Defence): I'm actually the one, Mr. Chair.

[*Translation*]

The Chair: Go ahead, Ms. Martel.

Ms. Sophie Martel: Mr. Chair and members of the committee, on behalf of the Department of National Defence and the Canadian Armed Forces, thank you for inviting us to the Standing Committee on Access to Information, Privacy and Ethics.

My name is Sophie Martel, and I am the acting chief information officer. I am the functional authority responsible for the department's entire information and communication technology program. I ensure that National Defence and the Canadian Armed Forces have a reliable, secure and integrated digital environment that meets operational needs.

My team delivers information and communication technology to support the core functions of defence, which are intelligence, surveillance, reconnaissance, communications, cyber-warfare, command, management and cybersecurity. The defence chief information officer is also responsible for the development and operational availability of the cyber-force within the Canadian Armed Forces cyber-command.

[*English*]

I'm joined today by the director general of cyber and command and control information systems operations, Brigadier-General Yarker.

Brigadier-General Yarker is responsible for the organization and execution of cyber operations and exercises within the Canadian Armed Forces, including the digital forensic function and the maintenance of key national command and control infrastructure.

I would like to emphasize that the protection of personal information is a top priority, and the Department of National Defence is committed to doing everything possible to protect that information. However, there has to be a balance. There's only a limited expectation of privacy when using our IT systems and mobile devices because they are subject to monitoring for the purposes of system administration, maintenance and security, and to ensure policy compliance.

Our monitoring is compliant with applicable government policies and standards.

[*Translation*]

In conclusion, I wish to reiterate that the Department of National Defence and the Canadian Armed Forces will continue to deliver on their mandate while protecting personal information.

[*English*]

My colleague and I would be pleased to address any questions you may have. As a matter of policy and to ensure operational security, we cannot disclose details on the use of specific equipment or on systems used operationally.

Thank you.

● (1105)

[*Translation*]

The Chair: Thank you, Ms. Martel. You did not use all your speaking time. It's good for the committee, which will be able to ask more questions.

Mr. Brisson, you have the floor for five minutes for your opening remarks.

Mr. Francis Brisson (Assistant Deputy Minister and Chief Financial Officer, Department of Natural Resources): Good morning, and thank you very much.

Thank you for this opportunity to speak about Natural Resources Canada's use of technological tools to safeguard our technological and data assets and ensure the consistent evolution and growth of our scientific endeavours.

I would like to recognize that I am speaking to you from the traditional unceded territory of the Algonquin Anishinaabe people. We recognize Indigenous peoples as the customary keepers and defenders of the Ottawa River watershed and its tributaries. We honour their long history of welcoming many nations to this beautiful territory and uphold and uplift the voice and values of our host nations.

[*English*]

As noted, I am Francis Brisson, the chief financial officer and assistant deputy minister responsible for corporate management services at Natural Resources Canada. My primary responsibilities include corporate services, human resources, information technology and security. Our department's chief information officer and CIO, Pierre Pelletier, who is here with me today, is responsible for the management, implementation and usability of information and computer technology at NRCan.

NRCan is both a science-based and a policy and economic organization. It is critical for NRCan to ensure its core functions remain resilient and responsive to internal and external threats. Threats affect not only our digital data but also our physical systems and devices. As the complexity of our digital environment grows, so does the risk of compromising our systems and assets. These risks include data breaches, intellectual property theft, service disruptions, financial setbacks and security threats.

Protecting against and responding to risks requires regular and sustained effort. Our department, like others, has many different systems, policies and tools to manage and respond to risks. Addressing and responding to threats can require forensic software tools. NRCan purchased a licence for magnetic forensics to have this tool in our tool kit, but we have never used it.

I would also underline that should the department have business requirements to use this software or similar software, NRCan will follow protocols and requirements for appropriate use and privacy impact assessments.

[*Translation*]

Thank you for your attention. Pierre Pelletier and I are pleased to answer your questions about our work.

The Chair: Thank you, Mr. Brisson. You also took less time than anticipated. That's good. The committee members will have more time to ask their questions.

We'll start our first round of questions.

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

[*English*]

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

Thanks to our witnesses for joining us here today.

Certainly I, as well as members of this committee and many Canadians, were concerned when the reports in the media came out that what would be, I think, accurately interpreted as quite invasive technology was being used. Certainly there was concern, which has led to the point we're at today, in light of some erosion of trust that has taken place in regard to governmental institutions over the last number of years in particular.

I do have a couple of questions. I'm going to start on the privacy impact assessment side of things. I'll ask this to both departments.

We heard from the commissioner last week that neither of your departments has submitted privacy impact assessments. Perhaps you could, in about 30 seconds—and I'll start with DND, and then go to NRCan—describe to me where that is at, whether or not you have submitted the privacy impact assessments, and whether or not you plan to?

DND, I'll start with you.

Ms. Sophie Martel: Thanks for the question.

We have a number of privacy impact assessments on the go right now. From a CIO point of view, as we are responsible for the security of our network, we follow the FAA, the standards of Treasury Board and all the laws. Outside that, if there's a need for a PIA, we actually work on it. For example, at this point in time we're looking at Microsoft 365, because we're starting to record information and do transcripts, and we're starting to look at what this will imply from a PIA point of view.

● (1110)

Mr. Damien Kurek: If I'm interpreting that correctly, the process is ongoing, but you have not submitted to the Information Commissioner a PIA regarding observation of devices?

Ms. Sophie Martel: Currently, a number of them in the department are ongoing.

Mr. Damien Kurek: Okay.

NRCan...?

Mr. Francis Brisson: Good morning.

From our perspective, like we said at the beginning in our opening remarks, we did purchase the tool. It was a tool we've purchased to have in our tool kit, and we have not used it from our perspective. One thing I wanted to reiterate and assure the committee of is that, should we plan on using the tool, that would be done only through a security mandate and clear protocols would be followed. Should we be using the tool, we will be doing a PIA from our perspective should that be the case.

At this point, we haven't used it. Should it be used further to an approved mandate from our chief security officer, we'd look at doing a PIA as we moved forward.

Mr. Damien Kurek: I appreciate that. I think one of the concerns we've heard is about a little bit of a disconnect. We had the commissioner last week talk about how he's happy to work with departments and agencies, yet had not received PIAs. Especially in light of hearing NRCan has procured software that would be capable of doing this, certainly, I would hope that the PIA process is ongoing and even could be done prior to the procurement of such software.

When it comes to tools capable generally of extracting personal information—I'll start with NRCan—has your department used a tool like that in the past?

Mr. Francis Brisson: From an NRCan perspective, we have tools and we have to monitor our system and so forth from that perspective. We ensure we are respectful and we support the policies around all of that. From our perspective, there are tools we are using to ensure we gather information, but it's done in the context of TBS policies and so forth.

Mr. Damien Kurek: Has information ever been gathered from people who are outside of the organization? I'm not talking about employees, but from people outside of the NRCan organization. Has information ever been gathered using these sorts of tools by your department?

Mr. Francis Brisson: The tool we've talked about, the forensic, has never been used, and should it be used, it would only be used internally. All the monitoring systems we have from our perspective in that space are used for internal purposes for within the organization and for administrative purposes in line with security requirements following a clear security mandate as we move forward.

Mr. Damien Kurek: I'll ask the same question to DND, and could I get it in 30 seconds or so?

Ms. Sophie Martel: Yes. In 30 seconds, we investigate networks, not people. In order to investigate networks, we do need to use tools to ensure the confidentiality, the integrity and the availability of data. That's following the FAA, the Treasury Board standard and the Privacy Act.

Mr. Damien Kurek: Has it ever been used on anybody outside of DND or the Canadian Armed Forces?

Ms. Sophie Martel: It's used to monitor our network, only our network.

Mr. Damien Kurek: Thank you.

I guess this is unsolicited advice, but especially in light of some of the media reports that have come out on this, I would hope there's a more proactive approach across departments and governments. The Information Commissioner wants to work with departments. Rebuilding some of that trust that's been lost is certainly something I would encourage all those who are...and I'll probably say it again: Let's work hard to make sure we can rebuild that trust that needs to be there with Canadians.

Thank you.

The Chair: Thank you, Mr. Kurek.

Everyone's making my job really easy today. That was right on time.

Ms. Khalid, you have six minutes exactly, hopefully. Go ahead.

Ms. Iqra Khalid (Mississauga—Erin Mills, Lib.): Oh, oh! We all have wishful thinking, Chair.

Thank you so much to our witnesses for being here today.

What I'm hoping to do is to talk to each department individually, so my questions will be similar for both of you.

First and foremost, to National Defence, what is the purpose of a privacy impact assessment to you?

● (1115)

Ms. Sophie Martel: The purpose of the privacy impact assessment is to make sure that we protect the information of citizens.

Ms. Iqra Khalid: Do you think it is necessary for a privacy impact assessment to be conducted within your department to ensure the trust that democracy depends on to function?

Ms. Sophie Martel: I think privacy of information is absolutely key. We absolutely need to make sure that the confidentiality, integrity and availability of the data are protected. That's why we're also protecting our network to protect the information and to make sure that the information is used the way it needs to be used.

Ms. Iqra Khalid: Why are we reading reports that you have not conducted a privacy impact assessment?

Ms. Sophie Martel: In the department, we have a number of privacy impact assessments ongoing right now. We are currently, in the CIO group more specifically, working on one with Microsoft 365. We do have a few ongoing right now.

Ms. Iqra Khalid: Are you in touch with our Privacy Commissioner to help you through that process?

Ms. Sophie Martel: We have a team in National Defence that is in touch.

Ms. Iqra Khalid: What are some of the challenges that you and your department are dealing with to ensure that a PIA is conducted effectively?

Ms. Sophie Martel: I'm not in a position to speak to that. I'm the CIO, so I'm not in a position to speak to the relationship between that organization and National Defence. Others are in a position to speak to that.

Ms. Iqra Khalid: Are you surveilling Canadians?

Ms. Sophie Martel: We're not surveilling Canadians.

As I said, we're here to support Canadians. We're here to keep them safe. We're monitoring networks. We're not monitoring people.

Ms. Iqra Khalid: If you needed to surveil a Canadian, is there a legal process through which you would do that?

Ms. Sophie Martel: It's not our mandate at all, but if another department or organization needed our help there, that would have to be done through specific processes.

Dave, do you want to add a bit more on that?

Brigadier-General Dave Yarker (Director General, Cyber and Command and Control Information Systems Operations, Department of National Defence): We would not be called upon to surveil Canadians. That's not within our mandate or remit.

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

I'm moving on to NRCan with the same questions.

What is the purpose of privacy impact assessments to you?

Mr. Francis Brisson: From our perspective, similar to our colleagues in DND, privacy impact assessments are about protecting the information and ensuring that, from our perspective, the information we have is gathered the right way, we're using it the right way, we're protecting the integrity of the information and, as discussed previously, we're reinforcing trust across government and departments.

Ms. Iqra Khalid: How high does privacy rank within your department in terms of priorities as you conduct your operations?

Mr. Francis Brisson: It's definitely extremely important from our perspective.

Being new in the role—as Pierre is as well—it is something that's extremely important to us. We want to continue to monitor progress in that space as we move along.

Ms. Iqra Khalid: Why haven't you conducted a privacy impact assessment?

Mr. Francis Brisson: From our perspective, the tool has never been used. If we were to use it, we have PIAs ready to go and available should that be the case.

We would be using this only further to our security mandate and by ensuring we follow the right protocols, which we have in place. Should this tool be necessary to investigate, then we would do a privacy assessment prior to using the tool.

Ms. Iqra Khalid: Have you been in contact with the Privacy Commissioner on this privacy impact assessment challenge?

Mr. Francis Brisson: We have not on this one, per se. We have a team within the department that's responsible for this.

I can reassure you that we have been in constant communication and discussion with them. Pierre and I, being new to the department, want to continue the great work that's being done in that space. We will continue to ensure that we're lining things up from that perspective.

● (1120)

Ms. Iqra Khalid: Are you surveilling Canadians?

Mr. Francis Brisson: No.

Ms. Iqra Khalid: What are the challenges your department faces in dealing with privacy when it comes to ensuring privacy for Canadians while also fulfilling your roles?

Mr. Francis Brisson: Maybe I can pass it to Pierre.

Mr. Pierre Pelletier (Chief Information Officer, Department of Natural Resources): Sure.

From a challenge perspective, it would potentially be how heavy the bureaucracy would be if, let's say, the Privacy Commissioner would require a specific, full-fledged PIA for an investigation. Departments are expected to have some degree of control within what's called the personal information bank. Within a workplace environment, you're expected to have some data that is shared with your employer. Most of the investigations would fall within what's accepted within a personal information bank. If anything goes beyond that mandate and scope, that's where a PIA would be required. A PIA should be very specific, and usually departments are well within the security protocol to work and support these operations.

The Chair: Thank you.

Mr. Pierre Pelletier: Having a good understanding of what that entails as we evolve the policy will support this guidance.

The Chair: Thank you, Mr. Pelletier.

[*Translation*]

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

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

I want to thank all the witnesses for being here. I'll ask both departments the same questions, starting with National Defence.

Ms. Martel, has your department purchased tools to collect data from mobile devices or computers?

Ms. Sophie Martel: As I said earlier, we purchased tools to protect our networks.

Our mandate is to protect and secure the confidentiality, integrity and availability of data on our networks. We purchased tools to investigate networks, not people.

Mr. René Villemure: What are these tools?

Ms. Sophie Martel: I would like Mr. Yarker to answer this question.

BGen Dave Yarker: We have a number of tools of this nature, but I won't go into them all today. As we said earlier, we have operational concerns related to security and our tools.

Mr. René Villemure: In short, what were the tools purchased for?

Ms. Sophie Martel: We purchased them to investigate the networks and for the networks.

Mr. René Villemure: There are people on the networks.

Ms. Sophie Martel: Yes. We agree that collecting information on the network means collecting data packets and personal information. That said, there are strict procedures for handling this information. People have received the necessary training and security clearance. They follow these strict procedures.

Mr. René Villemure: The privacy impact assessment wasn't done in this case, right?

Ms. Sophie Martel: As part of the work to protect our networks, we comply with the Privacy Act, the Financial Administration Act and all relevant Treasury Board standards.

We're also looking at the need for a privacy impact assessment. We started this type of assessment in the case of Microsoft 365.

Mr. René Villemure: Do you agree with the Privacy Commissioner of Canada that some departments and agencies, including yours, are violating certain administrative provisions of the Privacy Act?

Ms. Sophie Martel: We currently use these tools in compliance with the Financial Administration Act, the Privacy Act and all Treasury Board standards.

Mr. René Villemure: Do you think that following the letter of the law is enough to generate trust?

Ms. Sophie Martel: We can ensure that people trust us. Our role is to protect the networks in order to protect Canadians.

Mr. René Villemure: You said something earlier that surprised me. When it comes to privacy, expectations are lower.

Ms. Sophie Martel: Sorry, could you repeat that?

Mr. René Villemure: You spoke about the expectation of privacy, which is lower in the case of a government device, for example, than…

Ms. Sophie Martel: I probably meant that, to use a government device and have a network account, employees must fill out a questionnaire. They know that they will be monitored for network security reasons.

Mr. René Villemure: Okay. Thank you.

I would now like to turn to you, Mr. Brisson, from the Department of Natural Resources.

As you said earlier, your department purchased tools but didn't use them. Why did you purchase the tools and why didn't you use them?

● (1125)

Mr. Francis Brisson: Thank you for the question.

Our department uses various tools, mechanisms and protocols. I must say that we don't always need to use these tools to conduct investigations. The department's internal investigations concern the actions of public servants, for example.

The various tools include our computer investigation tool, which is available as needed. This tool can help us speed up searches and gather information, for example. However, we haven't needed to use it for queries. That said, it's part of our toolbox.

Mr. René Villemure: You're ready.

Mr. Francis Brisson: If we were to use it, we would have the security protocol and the mandate to do so.

However, before using the tool, we would make sure to carry out a privacy impact assessment.

Mr. René Villemure: What level of authority is required to purchase this type of tool? Is it authorized by you, as deputy minister, or by someone lower or higher in the hierarchy?

Mr. Francis Brisson: To my knowledge, at the time, the tool was authorized by the chief information officer, Mr. Pelletier's current position, after a discussion with the department's head of security.

Mr. René Villemure: So there are certain requirements.

Mr. Francis Brisson: Yes, absolutely. We follow the protocols in place before proceeding. We purchased the tool through Shared Services Canada, after discussions, in keeping with the protocols and based on the information that we had.

Mr. René Villemure: What are you looking for? Employee misconduct?

Mr. Francis Brisson: The monitoring system makes sure that everything is in place. These tools are used if we have a security mandate to look at a case a bit more closely.

Mr. René Villemure: What are you looking for?

Mr. Francis Brisson: It involves determining whether someone is disclosing information that falls within the definition set out in our security mandate. We would then collect the information necessary to meet these needs.

Mr. René Villemure: Ultimately, it's about identifying misconduct.

Mr. Francis Brisson: Yes, that's certainly possible. There may be different reasons.

Mr. René Villemure: Thank you.

[*English*]

The Chair: Thank you, Monsieur Villemure and Monsieur Brisson.

Mr. Green, you have six minutes. Go ahead, please.

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

I begin my comments with Mr. Yarker. Would you agree that the spirit of this conversation is about trust?

BGen Dave Yarker: Yes. Certainly from our perspective, the tools and questions that we use and the processes that we wrap around them are deliberately intended to increase the trust in our network and to ensure that it's not compromised.

Mr. Matthew Green: I think it's safe to say.... Maybe I'll put this question another way. Those who are enrolled in the military, by virtue of their enrolment in the military, aren't exactly citizens. I wouldn't necessarily compare your members to members of the Department of Agriculture, for instance. Is that correct?

BGen Dave Yarker: Okay. I certainly understand your point. Thank you for the question.

What I would say is that all members of the department retain their right to appropriate privacy, and we certainly consider those in all of our operations.

Mr. Matthew Green: You did make a statement earlier, though, about it not being within your mandate to surveil Canadians.

BGen Dave Yarker: That's correct.

Mr. Matthew Green: In your role, are you a military intelligence officer?

BGen Dave Yarker: I am not. My role is as a cyber-operations officer, focused here largely on cyber-defensive operations.

Mr. Matthew Green: Have you ever had any dealings with Canadian joint operations command?

BGen Dave Yarker: Yes, I do work with Canadian joint operations command regularly.

● (1130)

Mr. Matthew Green: How closely?

BGen Dave Yarker: Very closely.

Mr. Matthew Green: Would you have worked with them at the time when they were surveilling Black Lives Matter, back in 2021?

BGen Dave Yarker: No, I have no knowledge of that.

Mr. Matthew Green: Again, when I talk about trust and the importance for Canadians watching to know the differences in who's mandated to do what, I find it quite shocking, quite frankly, that the Canadian military had a file on BLM, that they said they were surveilling local context for operations in Canada and that in the file they had deemed them hostile foreign actors.

As somebody who has been to many of those rallies and involved in that work, I can't help but think that maybe, at some point, I was surveilled in that way. If you're familiar with their operations, what technology would they have used to track the movements of a protest organization or protests across the country?

BGen Dave Yarker: I'm afraid that's beyond my remit. I don't know the answer to your question.

Mr. Matthew Green: Is there AI technology that's used, to your knowledge, to surveil online social media activity, or is that done manually through the joint operations command?

BGen Dave Yarker: I'm afraid I don't know the answer to that question.

Mr. Matthew Green: Is there any context in which your department—and Ms. Martel, feel free to jump in on this—would use open-source information collection for social media usages by the members of the Department of National Defence?

BGen Dave Yarker: Certainly, I would say that, within the context of cyber-defence, we would not do that. Again, when it comes to cyber-defence and the kinds of tools we're talking about here today, those tools and the use of them are focused on ensuring that we're secure.

Mr. Matthew Green: The question is outside of your scope. I'll take that.

As I mentioned when you came in, part of our work is being at the end of the line of questioning and picking up on things that were said. I'm just making sure that it kind of aligns with my past experiences. I'm still kind of startled by the military's use in that application. If you want to report that back to your superiors to know that's still a question I have here at the privacy and ethics committee, I would love to have an answer to that.

In this work, I know that we've tried to create a distinction between an on-device information collection tool, spyware, versus this kind of forensic use. Are there also on-device applications that you use in the Department of National Defence?

BGen Dave Yarker: Some of these tools will look at individual and point devices. That's sort of the purpose of the tool. However, if I understand the thrust of your question, these are things that we use to investigate security incidents. We don't use them for other purposes.

Mr. Matthew Green: Okay, so there's no ongoing monitoring that would happen.

BGen Dave Yarker: No. We definitely, across the network security infrastructure, have monitoring tools that monitor for malicious activity and the like.

Mr. Matthew Green: I'll get more specific.

Are you familiar with the technology called Pegasus?

BGen Dave Yarker: I am, yes.

Mr. Matthew Green: Is there anything like Pegasus—not the brand name but the application of it?

BGen Dave Yarker: Within cybersecurity and cyber-defence, we do not use those kinds of technologies, I believe, in the sense that you're asking.

Mr. Matthew Green: Would you have knowledge of its being used in the Department of National Defence?

BGen Dave Yarker: I don't have any knowledge of its being used in the Department of National Defence.

Mr. Matthew Green: That's fair enough. Thank you very much.

Heading down to both of you folks, we're making the distinction again between—and I think it's an important distinction to make—something that's used for forensic, which needs the actual physical device in hand as part of an investigation versus what is deemed to be spyware. I used the reference to Pegasus, but these are things that would be surreptitiously collecting data in real time all the time.

To your knowledge, do you ever use those types of applications within the application of federal devices?

Mr. Francis Brisson: We don't.

Mr. Matthew Green: What's the rationale then, just one more time for the sake of this committee, for the purchase of this type of forensic device?

Mr. Pierre Pelletier: It's to be effective in the event that there's a security issue.

Mr. Matthew Green: How often do these security issues come up? Do you have a report in your departmental reporting back that we had 36 of these incidents?

Mr. Pierre Pelletier: It's not something I have readily available. For security reasons and our ability as an organization to withstand any potential threat, I would not disclose this readily in a public forum. We do have internal data about this, yes.

● (1135)

Mr. Matthew Green: Okay. At a future date, if we went in camera, is that something we could discuss without the media and the public present?

Mr. Pierre Pelletier: That's correct.

Mr. Matthew Green: Okay. Thank you very much.

The Chair: Thank you, Mr. Green and Mr. Pelletier.

That concludes our first round of questioning.

We're going to go to five, five, two and half, and two and half, starting with Mr. Brock.

Go ahead, sir.

Mr. Larry Brock (Brantford—Brant, CPC): Thank you, Chair.

Thank you, witnesses, for your attendance today.

I want to start by looking at first principles. This study essentially arose after a report by the CBC late last fall on how the Government of Canada and various departments—two of which are before the committee today—had used software and hardware to spy not only on the federal public service but on Canadians.

We found out about this particular incident probably years after the fact, and the information was obtained through an ATIP request by a professor at York University, an expert in privacy, who had some concerns about the ability of government officials to spy on employees and Canadians. He received information regarding the contracts—there were two contracts with the departments—he was reviewing. Radio-Canada received these contracts, and Radio-Canada reached out to both the departments for an explanation regarding their use of this spyware.

I wanted to lay the ground rules out, because I think doing so is important for the first question I will pose, which will be for National Resources. There appears to be a little bit of a disconnect, and I want you to help explain this particular issue. Radio-Canada reached out to your department. I don't know who it was in particular, but your department confirmed that you had the software, you had the hardware, but you had not provided the PIAs in relation to that. That's one issue.

Then I saw in a report by the CBC following the appearance of the Privacy Commissioner—this was in a report dated February 2—that National Resources Canada told the commissioner, after his appearance I would imagine, that it had bought the data extraction tools but never used them.

Why then would you tell Radio-Canada you did this, but you've never used PIAs, and then conversely tell the commissioner that you had the tools but never used them? Do you see a bit of a disconnect there?

Mr. Francis Brisson: Thanks for the question. Hopefully I have understood it.

From our perspective, I'll state the facts as I know them, and hopefully that will address your understanding.

We purchased the tool and we have it, and from my understanding we've had it since 2018. The tool has been available to us but has never been used. We don't have anyone in the department right now who can use it, and if we were to feel that, based on a security situation we would need to use a tool like this, based on a clear mandate, then from there we would automatically turn around and fill in a PIA to ensure that we were doing things the right way.

From our perspective, we've never used it, and if we were to use it, given the need from a security perspective, we would automatically do a PIA.

Mr. Larry Brock: Over the years your department has probably had instances of employee misconduct. Would that be fair to say?

Mr. Francis Brisson: I cannot speak for—

Mr. Larry Brock: Can either of you speak to that issue?

Mr. Pierre Pelletier: I think it's fair to say so, yes.

Mr. Larry Brock: In the course of those investigations, did you ever use software and hardware similar to the ones we're talking about today?

Mr. Pierre Pelletier: It's possible, but you wouldn't necessarily need to have the tools. The tools help enhance our ability, but it could be done manually.

● (1140)

Mr. Larry Brock: When you used other tools, did you file a PIA?

Mr. Pierre Pelletier: We did not to my knowledge, but within the framework on privacy impact assessment, departments have the ability to work within what is called personal information banks. Those contain predetermined types of information that we as a department would want to access from our employees. It is my understanding that, when we work within that set of information, we are within our mandate.

Mr. Larry Brock: Do you understand that there's a directive by the Treasury Board—

Mr. Pierre Pelletier: That's correct.

Mr. Larry Brock: —that PIAs need to be adopted across the board?

Mr. Pierre Pelletier: On the programs, that's correct.

Mr. Larry Brock: Yes, you are aware of that.

Mr. Pierre Pelletier: NRCan has that.

Mr. Larry Brock: Thank you, and I'm out of time.

Thank you, Chair.

The Chair: Thank you, Mr. Brock.

We have Mr. Bains for five minutes.

Go ahead, please.

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

Thank you to our guests for joining us today. You all have very important roles to play.

My first question is for the Department of Natural Resources. Do you believe the data, assets and lab systems that NRCan operates are protected and secure?

Mr. Francis Brisson: Yes. From our perspective, this is our mandate, and we do what we can to monitor and ensure that they are protected.

Mr. Parm Bains: What do you do to make sure that they're protected? How do you monitor and protect that?

Mr. Francis Brisson: I can turn it to Pierre.

Mr. Pierre Pelletier: We work with our service provider. We work closely with Shared Services Canada to make sure that the network is monitored and protected. Similarly, we work with our central agencies to support it from a cybersecurity threat perspective, and we maintain this equipment. We keep it up to date. We provide guidance on utilization of the network. We keep and maintain our systems and patch them for security. We also internally train personnel to make sure they're following the proper security guidance.

Mr. Parm Bains: You mentioned NRCan is adapting to an increased focus on security. Can you elaborate on some of the threats facing Canada?

Mr. Pierre Pelletier : There are many threats. A lot of what NRCan works on has commercial value, so there's an external threat, for sure. That's always the case.

Mr. Parm Bains: Is that to our natural resources in general?

Mr. Pierre Pelletier: There are many areas of business, such as energy, where NRCan is interesting for foreign entity or domestic reasons. It is always the nature of the business. The interesting challenge within NRCan is the open nature of the science culture. It's definitely a challenge for us to maintain the proper balance of sharing information with key stakeholders and protecting important assets.

Mr. Parm Bains: You mentioned domestic. Can you share what the domestic threat is?

Mr. Pierre Pelletier: From a commercial perspective, there's an interest in some of the technology, the breakthroughs or the scientific information that would have potential—

Mr. Parm Bains: Do you mean intellectual property, things like that?

Mr. Pierre Pelletier: That's correct.

Mr. Parm Bains: What circumstances occurred that warranted the procurement of this offer?

Mr. Pierre Pelletier: It was mostly from a readiness perspective. As an IT organization, I think it's perfectly normal for us to keep up to date and stay current with the technological advances. The technology is always advancing and evolving. The threat vectors are also advancing and people get more sophisticated, so I think it's properly normal for an organization to make sure that it maintains a certain degree of technology savviness.

Mr. Parm Bains: How often are you reviewing? Is this just constant?

Mr. Pierre Pelletier: That's correct.

Mr. Parm Bains: Are government employees made aware of when the forensic tools are used during investigations? I think that question may have been asked slightly differently.

Mr. Pierre Pelletier: IT security would be engaged via a well-established protocol, so our chief security officer would initiate a mandate on investigation. That's where IT gets engaged. From my perspective as a CIO, my mandate focuses on providing tools and equipment to help support a security investigation. Absolutely, there is an established protocol, and specifically to—

● (1145)

Mr. Parm Bains: Can you give an example maybe?

Mr. Pierre Pelletier: Absolutely. If we were to investigate a physical device, this would be done, first of all, within a personnel security engagement. At this stage, they would absolutely do a review of the impact on security, and they would engage the scope of the actual investigation. IT would get engaged. This is done in a secure environment where access is logged and managed. The information provided by IT is returned to the chief security officer organization, and that's where it's treated internally.

Mr. Parm Bains: How much time do I have?

The Chair: You have 15 seconds.

Mr. Parm Bains: Okay. Thank you very much for your time.

The Chair: Thank you, Mr. Bains.

Thank you, Mr. Pelletier.

[*Translation*]

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

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

Ms. Martel, Mr. Pelletier said earlier that there were other ways to achieve the same results. Is that also true for you?

Ms. Sophie Martel: You mean other ways to achieve what, exactly?

Mr. René Villemure: I'm talking about other ways to achieve the same results.

Ms. Sophie Martel: Can you provide a bit more information?

Mr. René Villemure: Are there other less invasive ways to achieve the same results?

Ms. Sophie Martel: Right now, we're using the tools needed to keep our networks secure. Most of these tools are as non-invasive as possible.

Mr. René Villemure: Can you elaborate on this?

Ms. Sophie Martel: Mr. Yarker can provide a further explanation.

[*English*]

BGen Dave Yarker: We would move to more invasive tools only if something about the nature of the investigation forced us to do that. Yes, we always turn to the least invasive tools possible.

[*Translation*]

Mr. René Villemure: Okay. Thank you.

Mr. Pelletier, my colleague asked you earlier whether employees know that they're being investigated with these tools. I imagine that, when people start working for you, they fill in all sorts of forms that authorize certain things. However, is that the same as clicking “I accept” when you visit a website but don't read the terms of use?

Mr. Pierre Pelletier: The government is no different from any other organization. When you use government networks, you have certain obligations as an employee to ensure that your use of the equipment complies with government policies. Clearly, a forensic analysis in particular can't be carried out without the knowledge of the people involved. Under no circumstances could we carry out a forensic analysis without first informing the people involved.

Mr. René Villemure: Like you, I think that makes sense, but are employees regularly reminded about security?

Mr. Pierre Pelletier: Absolutely. A reminder pops up automatically every time someone connects to the virtual private network. The department regularly reminds employees of their obligations. In fact, we’re in the middle of cybersecurity month. Our department is therefore taking steps to make employees aware of this reality.

Mr. René Villemure: So, if you ended up using that particular tool, people wouldn’t be able to say they had forgotten or didn’t know it could be used. In other words, they were informed.

Mr. Pierre Pelletier: If we were to use that particular tool, it would be with a great deal of transparency with the organization and the employee involved.

Mr. René Villemure: Very well. Thank you very much.

The Chair: Thank you, Mr. Villemure.

[*English*]

Mr. Green, you have two and a half minutes.

Mr. Matthew Green: Thank you.

I'm going to go back to my friend, Mr. Yarker. I want to have, in fairness, the opportunity for the public to get a sense of what risk Canada is under in terms of cybersecurity and cyber-threats.

In a succinct way, can you express the importance of the work that you do in terms of protecting our country from foreign attacks and possible disruptions, including very serious military breaches?

BGen Dave Yarker: Certainly. Thank you for the question.

We know very well that cyberspace is not a friendly space. Cyberspace is a place where we face numerous threats from various directions—both nation-states and criminal actors. We take those threats very seriously.

Within the Department of National Defence, we have a robust cybersecurity program. On top of that, we have cyber-forces capable of defending our networks when and where necessary.

Mr. Matthew Green: In some way, it's like a fourth dimension to the typical, traditional military operations. It's a complete new world with technologies that surpass most people's imaginations.

Is that fair to say?

● (1150)

BGen Dave Yarker: Yes. Thank you for the question.

I would say that we certainly treat it as another domain. We have air, land, sea and space. Cyber is one of those.

Mr. Matthew Green: Do you feel adequately prepared for what's out there?

BGen Dave Yarker: Cyberspace, as I've mentioned, is a bit of a nasty place. It's also a place where we are learning, and there's an awful lot to continue to do.

Although, yes, we have well-trained, well-prepared forces, it's also a space where there is always more work left to do.

Mr. Matthew Green: I thank both you and Ms. Martel for your service to the country.

I'm going to go over to you fellows at the end of the table around the privacy impact assessment, recognizing that you haven't had to use it. What I'm trying to get out of this study, in terms of the real legislative value of it, is what the process, the systems and the steps it takes are.

You said that you bought the tech and you're prepared to use it if you need it. You said that you would do a PIA if you needed to use the tech. Why not do it in advance?

Mr. Francis Brisson: Definitely. From our perspective, as I discussed before, Pierre and I are new in the role, and this is definitely something we want to continue exploring and looking into further.

Mr. Matthew Green: Do you have the ability, the decision-making capability, to go from this meeting and just start a PIA, or is that something you have to...?

Mr. Francis Brisson: No. From our perspective, we definitely can.

Mr. Matthew Green: Is that something you will commit to doing after leaving this committee?

Mr. Francis Brisson: From our perspective, I have no problem doing this because we are proactively looking at what we can do in that space. I feel comfortable doing so given that we have the—

Mr. Matthew Green: I will take that as a commitment. I appreciate it.

The Chair: Thank you, Mr. Green and Mr. Brisson.

We have time for four and four. We are going to go to Mr. Barrett. That will take us to near the top, and then we will switch over to our next panel.

Go ahead, Mr. Barrett.

Mr. Michael Barrett (Leeds—Grenville—Thousand Islands and Rideau Lakes, CPC): Let's clarify here. There was the article that was referenced by my colleague before from the CBC. The story was from November 29, 2023. The article was “Tools capable of extracting personal data from phones being used by 13 federal departments, documents show”. Those departments listed include your departments.

General and Ms. Martel, does your department have that capability—yes or no?

Ms. Sophie Martel: Yes. We have the—

Mr. Michael Barrett: Okay. You have the capability.

You said that you don't monitor individuals. You only monitor networks.

Ms. Sophie Martel: That's correct.

Mr. Michael Barrett: The tools capable of extracting personal data from phones, how is that monitoring a network and not monitoring an individual?

Ms. Sophie Martel: I'm going to let Dave answer that one.

BGen Dave Yarker: If you take a look at a typical cyber-defence incident, which is really what we're talking about here, the kinds of tools we're talking about are the tools that you would need to figure out how and why a device like a cellphone had been compromised.

Mr. Michael Barrett: Okay.

BGen Dave Yarker: I think our point is that the angle we come at it from is the compromise of the device and the network.

Mr. Michael Barrett: Right. In your investigation, one of your investigative tools is to access an individual's phone. You would use this software as a tool, and part of your process would be to access an individual's phone.

Give a quick yes or no. I have limited time.

BGen Dave Yarker: Only National Defence devices are used, but obviously, those devices are used by individuals.

Mr. Michael Barrett: Okay. I don't think that was clear in your initial responses.

Do members have a right to privacy?

Ms. Sophie Martel: Absolutely. Yes.

Mr. Michael Barrett: Have you used this capability on members' phones?

BGen Dave Yarker: Their personal phones...? No.

Mr. Michael Barrett: On phones assigned to members...?

BGen Dave Yarker: Yes.

Mr. Michael Barrett: Are members allowed to log into personal cloud-based accounts on issued phones?

Ms. Sophie Martel: They are not supposed to, but some do.

BGen Dave Yarker: Yes.

Mr. Michael Barrett: Is it a violation of their terms of employment to do that?

Ms. Sophie Martel: The government—

Mr. Michael Barrett: The general said yes, and you said no, so there's obviously a disagreement even at the table. I would expect that if you surveyed members they might have differing ideas if we're not even sure at this level.

Ms. Sophie Martel: I'm going to explain myself.

As I said earlier, when we get an account on the network, to reach the account you need to sign to say that you will only use that device to do government work.

Mr. Michael Barrett: Sure.

Ms. Sophie Martel: Now, will people—

Mr. Michael Barrett: To do government work on these phones people use messaging applications. Those messaging applications are usually the same application they use on their personal device, which would give you access to the personal information on their device.

Did you get a PIA before you first used this technology?

● (1155)

Ms. Sophie Martel: Before we first used.... What we are doing with a PIA is making sure that we follow the FAA and the Treasury Board standards.

Mr. Michael Barrett: Did you complete the process prior to first using it?

Ms. Sophie Martel: We completed the process that needed to be completed based on government policies and standards to do our business, which is network security.

Mr. Michael Barrett: You don't believe that you need to do a PIA before using it.

Ms. Sophie Martel: No, what I'm saying is—

Mr. Michael Barrett: The question is very clear, Madam.

Did you or did you not complete a PIA before first using this tool? You did, or you didn't.

Ms. Sophie Martel: I'm not sure to be honest with you.

BGen Dave Yarker: We did not.

Mr. Michael Barrett: Okay. My question is why you think that you don't need to do it, but I'm out of time.

Your members are Canadian citizens. Canadians by your agreement have a right to privacy, and your failure to undertake a PIA is a failure to safeguard and respect the privacy of your members.

I'm sorry that I don't have more time to continue.

The Chair: Thank you, Mr. Barrett.

Mr. Kelloway, you have four minutes. Go ahead, please.

Mr. Mike Kelloway (Cape Breton—Canso, Lib.): Thank you, Mr. Chair.

My questions are for National Defence.

During the course of your testimony, you indicated that DND's usage of digital forensic tools complies with government policies and standards, and they are only used on an internal basis. Then, upon being issued an official departmental device, are DND employees clearly advised that their devices are subject to forensic digital tools?

Ms. Sophie Martel: Yes, they absolutely are. We also send a reminder every time someone logs into the system so they're made aware of this. Yes, they are.

Mr. Mike Kelloway: Thank you for that.

Considering that National Defence officials deal with matters of the utmost national security on their official devices, do you consider it an essential security measure that DND employees are subject to digital monitoring when using their official devices?

BGen Dave Yarker: I would say, from a security perspective, that we monitor the network, as I mentioned, for security threats, compromises and the like. We are absolutely aware that some senior leadership are more likely to be targeted by threat actors.

Mr. Mike Kelloway: Thank you for that. I appreciate it.

To either of you, do you know of any other national defence or national security entity within our country, or for that matter any allied nation, that ensures total privacy for employees who handle national security information?

Ms. Sophie Martel: We ensure total security of privacy of employees using our system. I mentioned that part of the reason we're doing network security is to ensure the confidentiality, integrity and availability of the data. We're working with our allies to make sure that the standards that we follow here are also standards that are followed in other countries.

Mr. Mike Kelloway: Thank you for that.

Mr. Chair, how much time do I have left?

The Chair: You have a minute and 45 seconds, but I'm going to give you an extra half-minute because Mr. Barrett took an extra half-minute.

Mr. Mike Kelloway: That's very kind of you. I appreciate it.

I'm going to pivot to Natural Resources, if I can.

I'm hearing today that your digital tools were procured through Shared Services Canada and that they've never been used. I'm wondering at what point in time the department determined that a requirement existed to procure these services through Shared Services Canada.

Mr. Francis Brisson: If I may, from our perspective, as suggested earlier and to reinforce that point, from what we understand, the department decided to purchase this to ensure that we had the tools necessary should we need them at a certain point in time. From our perspective, that's what we've done.

Since then, on a yearly basis, we renew our licence in case it's needed. As I suggested before, should we ever decide to use it in line with a security requirement, we'd ensure that we looked at doing a PIA. However, as committed earlier, this is also something that we'll look at doing as we move forward, even if it's not being used.

Mr. Mike Kelloway: I have one last question, if I have the time.

During the course of your testimony, Mr. Brisson, you indicated that Natural Resources uses forensic digital tools in order to mitigate threats. Are these threats solely with respect to the department's own internal systems, or does this include threats relating to Canada's natural resources?

● (1200)

Mr. Pierre Pelletier: That's a really good question. I would argue that it's mostly related to the data that are transiting within NRCan's business—the science and the research associated with it. For natural resources, it's outside of my ability to answer. I do not know.

Mr. Mike Kelloway: Thank you, Mr. Chair.

The Chair: Thank you, Mr. Kelloway.

[*Translation*]

On behalf of the committee, I want to thank the witnesses from our first panel: Mr. Yarker, Ms. Martel, Mr. Brisson and Mr. Pelletier.

We will suspend the meeting for a few minutes to set up the next witness panel.

● (1200)

(Pause)

● (1205)

[*English*]

The Chair: Welcome back, everyone.

We're going to start our second panel.

As a reminder to all our witnesses, please be mindful of the earpieces. Keep them away from the microphones when you're speaking to protect our interpreters from any hearing damage.

[*Translation*]

I would like to welcome the witnesses appearing during the second hour of our meeting today.

[*English*]

From the Canada Border Services Agency, we have Mr. Aaron McCrorie, who is the vice-president, intelligence and enforcement. From Correctional Services Canada, we have France Gratton, assistant commissioner, correctional operations and programs, as well as Tony Matson, assistant commissioner and chief financial officer, corporate services.

From the Royal Canadian Mounted Police, I want to welcome Mr. Bryan Larkin, who is our deputy commissioner, specialized policing services, and Nicolas Gagné, superintendent, Royal Canadian Mounted Police.

We're going to start with opening statements of five minutes.

Mr. McCrorie, I understand that you are going first. You have five minutes. Please start.

Thank you.

Mr. Aaron McCrorie (Vice-President, Intelligence and Enforcement, Canada Border Services Agency): Thank you, Mr. Chair.

As stated, I am Aaron McCrorie. I am the vice-president for intelligence and enforcement at the CBSA. It's a pleasure to be here today.

Beyond the CBSA's role of processing people and goods at the physical border, the CBSA is responsible for enforcing Canada's border legislation, including the Customs Act and the Immigration and Refugee Protection Act.

This responsibility includes conducting criminal investigations into alleged offences under border legislation. It is within this investigative purview that the CBSA uses digital forensics hardware and software in order to unlock and decrypt seized digital devices and subsequently search for evidence of offences. I like to think of it as using a locksmith to open a locked box that has evidence within it.

Devices examined by the CBSA's digital forensics teams have been seized pursuant to specific court orders such as search warrants or judicial authorizations issued to CBSA investigators. The data extracted from seized digital devices is processed only within the CBSA's own digital forensic laboratories and is provided only to those having lawful authority to access that data.

We are currently governing our use of this using the privacy information bank, which outlines clearly the types of information that we are gathering and the uses that we put it to.

We are also in the process of working with our internal partners on a privacy impact assessment. We started that work in 2020. Unfortunately, it was delayed for a number of reasons. We are continuing that work and will be engaging with the Office of the Privacy Commissioner to finalize that privacy impact assessment.

I'd also like to clarify that spyware is typically defined as software installed in a device for the purposes of covertly intercepting, monitoring and/or gathering a user's activities or data. I want to assure the committee and the Canadian public that digital forensic tools utilized by the CBSA's investigators are not spyware. We use digital forensics hardware and software to unlock and decrypt seized digital devices as an important tool in our efforts to enforce border-related legislation and to protect Canadians.

I want to assure the committee members again that only properly trained investigators acting with judicial authorization use this technology.

Thank you for the opportunity to appear before you. I will be happy to answer any questions you may have.

● (1210)

The Chair: Thank you, Mr. McCrorie.

Next, we'll go to Ms. Gratton.

Please go ahead for up to five minutes.

[*Translation*]

Ms. France Gratton (Assistant Commissioner, Correctional Operations and Programs, Correctional Service of Canada): Hello everyone.

Mr. Chair and members of the committee, thank you for the opportunity to appear before you today as part of your study.

My name is France Gratton, and I am the assistant commissioner for correctional operations and programs with the Correctional Service of Canada. With me today is Tony Matson, assistant commissioner for corporate services and chief financial officer.

Protecting the safety and security of our institutions and our communities while promoting the safe rehabilitation of offenders remains our biggest priority.

By its very nature, managing offenders poses various challenges, including the ongoing threats posed by the introduction and circulation of contraband. Contraband is defined as any item that could jeopardize the security of the institution or the safety of persons when that item is possessed without prior authorization.

[*English*]

As per our legislative authority, contraband such as electronic devices will be seized. In response to the risk posed by the presence of contraband cellular phones and illicit drugs, CSC must leverage technologies to aid in detection and in intelligence development.

In this context, CSC secured tools to extract digital information for intelligence purposes. We do not use these tools to conduct investigations on devices that are owned by staff, visitors or volunteers. Access to these tools is limited and controlled. The tools are used only on stand-alone computers that are not connected to any corporate network. Strict safeguards are in place to limit access to any extracted data.

In the past, CSC has undertaken the privacy impact assessment checklist on CSC's digital forensic activities. As the use of enhanced tools to combat criminal activity has expanded over the past few years, CSC has committed to renewing the initial assessment and to completing an updated checklist.

We remain committed to upholding our privacy obligations with established and appropriate safeguards in place.

Thank you. I welcome any questions that you may have.

[*Translation*]

The Chair: Thank you for your opening remarks, Ms. Gratton.

[*English*]

Mr. Larkin, you're next for up to five minutes. Go ahead, sir.

[*Translation*]

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

[*English*]

Good afternoon, Mr. Chair and honourable members of the committee.

I'm pleased to be joined by Superintendent Nicolas Gagné, who's the director of the RCMP's technical investigative services operational directorate.

We're also very grateful for the opportunity to speak to you today about the RCMP's use of tools that extract and analyze information from digital devices that are essential to modern-day policing.

First, I would like to acknowledge and confirm that the RCMP does use some of the digital forensic tools that were cited in the December 2023 CBC article, including both Cellebrite and Graykey, which is now also known as Magnet Forensics.

The media reports suggesting that these digital forensic tools are considered spyware are inaccurate, though, and I will clarify that through your questions.

These tools are used on digital devices that are lawfully seized through criminal investigations. They obtain and analyze data on a device that is in possession of the RCMP. We use judicial authorization, search warrants and general warrants required from the courts, specifying how, what devices and the time frame during which we can collect the information from these devices by trained and skilled investigators. These tools are not used in any way for surveillance and/or mass surveillance.

For criminal investigations, the RCMP only uses these tools to extract and recover data in support of its mandated activities under the following circumstances: prior judicial authorization from our Canadian courts and within the prescribed limits of the search warrant; voluntary consent from the device owner, such as a witness to a crime and/or the victim of the crime; and/or under exigent circumstances when it's not possible to obtain a warrant, as defined under the legislation of the Criminal Code of Canada.

For administrative investigations, the RCMP does have legislation and policies that govern our use. The lawful ability to request assistance from our digital forensics program does exist within our organization. The collection of evidence through these tools is based on necessity and proportionality to the allegations of the internal conduct investigation. We would only perform an examination on RCMP-owned devices, and any personal device would require a judicial warrant.

While these tools can allow full access to all the information on the device, only that which is specified in the warrant or relevant to the administrative investigation is provided to the investigators.

Despite the privacy protections in place, the RCMP recognizes the inherent privacy issues related to these tools and the need for transparency and accountability. In January 2021, we provided a technical briefing to the Office of the Privacy Commissioner on digital forensic tools, and a privacy assessment is currently under way and is expected to be completed by mid-2024.

Again, thank you for the opportunity to be here. We look forward to your questions.

● (1215)

The Chair: Thank you, Deputy Commissioner Larkin.

We're going to start with our first six-minute round.

Mr. Brock, you have six minutes. Go ahead, please.

Mr. Larry Brock: Thank you, Chair.

Thank you to the witnesses for your attendance today. I'm going to start by making some opening remarks.

This story broke as a result of an ATIP from a York University professor, an expert in privacy. The data was turned over to Radio-Canada. Radio-Canada reached out to your respective departments asking if you're using the software, confirming that you're using the software, and if you had first conducted privacy impact assessments. According to their written responses, as per Radio-Canada, none did.

My first question is for the CBSA.

When did you purchase the software, sir, from Shared Services Canada?

Mr. Aaron McCrorie: The first procurement of Graykey was in March 2019. The first purchase of Cellebrite premium units was in March 2021.

Mr. Larry Brock: How many times have you used this particular software in question?

Mr. Aaron McCrorie: I couldn't tell you exactly how many times we've used the software. What I can tell you is that, for example, in 2023, we had 119 criminal investigations during the course of which we seized 712 devices. When we say, "712 devices", that will include, for example, the memory card or the SIM card that's in the cellphone, so a cellphone could count as three devices.

Mr. Larry Brock: Will you table with this committee a number as to how many times you used this specific software from the date of purchase?

Mr. Aaron McCrorie: We'll do our very best. I can't assure you that we can count every single instance, but we can certainly give you stats.

Mr. Larry Brock: We're talking hundreds.

Mr. Aaron McCrorie: I'd say yes.

In 2021, we seized—

Mr. Larry Brock: We're talking about hundreds of investigations using this software and not once did your department seek out a privacy impact assessment. Is that correct?

Mr. Aaron McCrorie: We do have the PIB, which is the privacy.... I apologize—the acronym is slipping my memory.

Mr. Larry Brock: Is it the PIA?

Mr. Aaron McCrorie: It's a PIB.

We post online what types of information we are gathering, under what circumstances we're gathering it and how we're using it.

We've started our internal process to do a program-level PIA because we want to do it at the program level, not at the device level.

Mr. Larry Brock: You understand, sir, that the PIA is not optional.

Mr. Aaron McCrorie: Agreed.

Mr. Larry Brock: It's a directive by the Treasury Board.

Mr. Aaron McCrorie: Agreed.

Mr. Larry Brock: When the commissioner testified last week, the commissioner reached out to your department and specifically asked you when you were going to start conducting PIAs. Your response was that you're looking into it, or you were about to start it.

What was your actual response? Are you still looking into the use of this mandated process, or have you actually started as a result of this controversy?

● (1220)

Mr. Aaron McCrorie: As I noted in my opening remarks, we started the process to do a privacy impact assessment for the entire criminal investigations program in 2022. We're following our internal processes in doing so.

As a result of that, we are now moving forward with the PIA, which we'll work with the Privacy Commissioner on.

Mr. Larry Brock: We have an auto theft crisis in this country. It's reaching alarming rates—so much so that the government is conducting a summit, which I believe is happening this Thursday.

The CBSA is in charge of protecting our borders. Is that correct?

Mr. Aaron McCrorie: Amongst others...yes.

Mr. Larry Brock: Justin Trudeau's and this government's mismanagement of our federal ports has turned them into parking lots for stolen cars that then disappear overseas. For instance, the port of Montreal—where the majority of stolen cars leave Canada—only has five CBSA agents to inspect the massive volume of containers that leave each year, according to Le Journal de Montréal. They also have one X-ray scanner that constantly breaks down. The federal ports in Vancouver, Prince Rupert and Halifax tell a similar story.

According to Peel detective Mark Haywood, the CBSA checks "less than one per cent" of all containers leaving the country. We're talking thousands of containers leaving every week. Why?

With all the money the government is providing the CBSA, why are you contributing to this crisis—

Ms. Pam Damoff (Oakville North—Burlington, Lib.): I have a point of order, Chair.

What is the relevance to this study?

The Chair: Thank you for the point of order. I think I've mentioned before, Ms. Damoff, that I generally give a lot of latitude to members of Parliament. I expect that Mr. Brock will come back to where we're at.

Perhaps we'll find out. He has a minute and 31 seconds left.

Mr. Brock, go ahead, please. You have the floor.

Mr. Larry Brock: His title is "intelligence and enforcement". This question I'm posing to him is squarely within his ability to answer.

With the hundreds of millions of dollars that the government is transferring to the CBSA to assist you in doing your work to enforce and to inspect, why has the department been so derelict in its responsibilities to inspect these containers? This clearly sends a message to the criminal underworld and the organized crime units that Canada is a haven for this type of activity.

We have law enforcement right here who I'm sure are very frustrated with your lack of attention to this issue. Please explain to law enforcement why we only have five agents.

Mr. Aaron McCrorie: What I'd suggest is that, in fact, we are a key partner working with law enforcement across the country.

Over the last year, we participated in 14 different joint operations with local police in the Toronto area, for example. We're working very closely with police in Ontario and Quebec to take a risk-based approach to examining containers.

I think you can understand that it's completely impossible to search every single container entering or leaving a port—

Mr. Larry Brock: Why?

Mr. Aaron McCrorie: The sheer volume and numbers of the thousands of those containers—

Mr. Larry Brock: Ask for resources.

Mr. Aaron McCrorie: What we are doing is that we are taking a risk-based approach using intelligence that we get from our partners in law enforcement—

Mr. Larry Brock: We're telegraphing to the world that we're not inspecting the containers leaving and we're not inspecting the containers arriving. That's why we have a fentanyl crisis. We have the illicit, deadly drugs coming from Asia that are not being inspected at the ports in Vancouver.

Ms. Iqra Khalid: I have a point of order, Chair.

The Chair: Mr. Brock, the six minutes are up.

Thank you, sir.

Mr. Larry Brock: Thank you.

The Chair: Go ahead on your point of order, Ms. Khalid.

Ms. Iqra Khalid: I just wanted to bring up that, unless auto theft is being conducted by surveillance devices, I don't see how that's relevant, Chair.

The Chair: I appreciate that. Thank you.

Go ahead, Ms. Damoff.

Ms. Pam Damoff: Thank you, Chair.

Thank you to all of the witnesses for being here.

I'm just going to start with a rhetorical question. I'm wondering if Mr. Brock is suggesting that this software be used to combat auto theft. I didn't hear that work its way into his question.

Trade would come to a halt if we inspected every single shipping container that left Canada. Is that not correct?

Mr. Aaron McCrorie: If we inspected every single shipping container coming into the country and leaving the country, trade would come to a halt.

Ms. Pam Damoff: Thank you.

Moving on to what our study is actually about, I have just a quick question.

Mr. Michael Barrett: Chair, I have a point of order.

We had two Liberal members interrupt Mr. Brock because of his line of questioning. Then Ms. Damoff continued on the exact same line of questioning.

This isn't a question, Chair, about the Standing Orders or relevance. It's about looking to disrupt a member who rightfully has the floor, who is within his time and who is asking questions and giving an opportunity to respond.

We've seen this before. If we want the meetings to descend into pure chaos, that invitation can be accepted, but now that we've seen that there are games being played, I think that the disruptions from Liberal members need to end.

● (1225)

The Chair: Thank you, Mr. Barrett.

Again, we've been on this committee together long enough, all of us, to know that I generally give a lot of latitude to members to utilize their time in the manner in which they choose. We have subject matter experts in front of us. Yes, we are dealing with a subject. My expectation is that we are going to get back to where we need to go with that subject.

I don't like, frankly, these constant interruptions and points of order just because we don't like what somebody's saying or what a line of questioning is. That goes for all sides.

Ms. Damoff, you have five minutes and 22 seconds left. Please continue with your line of questioning.

You have the floor. Go ahead, please.

Ms. Pam Damoff: Thank you.

I need just very quick answers from all three of you. Maybe we'll start with the RCMP and work this way.

Is this software used on your employees' phones?

D/Commr Bryan Larkin: We do not use the software on employees' phones. We do have the ability to use it because our phones are deployed operationally. Each member signs a consent around user use, etc. However, we don't actively monitor them. It would be through a specific allegation relating to a code of conduct or a criminal investigation.

As I alluded to, if it's a criminal investigation, we will always seek judicial authority. If it's an internal code, then potentially the investigator will consult with digital forensics and make an assessment as to whether it's required or not.

Ms. Pam Damoff: Thank you.

Mr. Aaron McCrorie: Thank you for the question.

No. We use these tools only in the pursuit of criminal investigations related to our border mandate, always with the use of a judicial authorization.

Ms. Pam Damoff: Thank you.

Ms. France Gratton: The answer is no. We don't use the software on employees' cellphones. We use it only on seized, contraband cellular phones that would have been introduced into our institution illegally.

Ms. Pam Damoff: Thank you. My next question is for CBSA.

You talked about seized devices. If I'm going through security coming into Canada and I'm taken off to secondary screening and you seize my phone, is that an instance where you would use this software?

Mr. Aaron McCrorie: No.

There are two different situations at play there. When you're crossing the border, there are regulatory requirements in place that allow us to do a search. If there's a search of a cellphone, that is done manually with the co-operation of the person in front of us.

The use of this technology in my particular organization is part of criminal investigations that, more often than not, are taking place inland and are related to things like firearms smuggling or violations of the IRPA. That's related to, for example, violations of the Immigration Act and counselling people to misrepresent themselves in order to get new immigration documents.

Ms. Pam Damoff: When it's seized and reviewed manually, is this software not used?

Mr. Aaron McCrorie: No.

Ms. Pam Damoff: Okay. Thank you for that.

I think the RCMP might be best-placed to speak to this.

Can you explain the process you need to go through in order to get information from a cellphone? It's a criminal investigation. What is the process that you need to go through in order to use this software or anything else to access a phone?

Mr. Nicolas Gagné (Superintendent, Royal Canadian Mounted Police): The digital forensic examiner would first get a copy of the warrant—the judicial authorization—to see what is the scope. They would determine which tool to use, depending on capability. Those capabilities vary depending on the make, model and operating system. They would retrieve—as much as possible—an image of the device. Sometimes it's not possible. Sometimes it's not possible at all to retrieve anything. Once the information is retrieved, the digital forensic examiner would then narrow it down to the width and scope of the warrant.

That is the report that would be provided to the investigator.

Ms. Pam Damoff: There have been implications that this software is being used to access Canadians' phones. I think I'm hearing from all of you that the case is that, if this software is used for the general public.... We heard previously that there are employees who are subject to its use on their phones. None of you are in that situation, but I think, more broadly, Canadians can feel confident that you're not accessing their cellphones without following the proper judicial process.

● (1230)

D/Commr Bryan Larkin: That's correct. These tools are targeted to a specific device. For example, in 2023, we examined 6,452 devices—that could be a smart phone, tablet or computer—across the country, but those are with judicial authorization so there's actually a tangible piece of evidence that we have. As I alluded to, a witness or a victim of crime may share their consent because they want to provide evidentiary documentary.

Given the complexity of this, I would like to extend to the committee an opportunity. If you would like a technical briefing, Superintendent Nicolas Gagné and his team, at your convenience with the clerk, would be pleased to welcome you into an RCMP facility and we would take you through how we extract digital evidence with judicial authorization so you could understand the complexity, the skill set, the training and the work we do.

Ms. Pam Damoff: Thank you.

Actually, having been part of an RCMP technical briefing on another issue, I would love to take you up on that. I would encourage the chair to perhaps follow up on the committee's taking advantage of the offer we've just been given.

The Chair: Thank you, Ms. Damoff.

Just to advise the committee, if there is a desire, we would need a travel request on behalf of the committee to do that, which would be sent to the Liaison Committee. I believe the deadline for that is February 16. That's something for the committee to consider.

[*Translation*]

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

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

I will address all three organizations and ask them to answer me one after the other.

During the investigation by Radio-Canada, you said you had not conducted any privacy impact assessments. Did I understand correctly?

Let’s start with you, Mr. Larkin.

[*English*]

D/Commr Bryan Larkin: That is correct.

We're in the process of completing it. We met with the Privacy Commissioner in 2021. However, we expect our privacy impact assessment to be complete by 2024. We do not have one for digital forensic tools. We do have one for ODITs, which is actually posted on our website.

[*Translation*]

Mr. René Villemure: Thank you.

Mr. McCrorie, I’m listening.

[*English*]

Mr. Aaron McCrorie: We use the personal information bank for now to demonstrate what information we're gathering and how we're using it, and we're in the process of doing a PIA, which we aim to have done.... It will probably be a little longer than for the RCMP, but we're aiming to have it done in co-operation with the OPC.

[*Translation*]

Mr. René Villemure: So it’s ongoing, but it’s not finished.

[*English*]

Mr. Aaron McCrorie: Exactly.

[*Translation*]

Mr. René Villemure: Ms. Gratton, over to you.

Ms. France Gratton: Once the software was purchased in 2010, we conducted a series of checks to determine if a privacy impact assessment was required. Based on the program we were setting up, the tool we were using and the way the information was going to be managed, it was not considered necessary.

Mr. René Villemure: I see. Is that the answer you gave Radio-Canada during its investigation?

Ms. France Gratton: Yes, we responded by saying that we had followed the list of checks in line with a privacy impact assessment.

Mr. René Villemure: Mr. McCrorie, did you say the same thing to Radio-Canada as part of its investigation, meaning that you were following the process, or did you say no?

[*English*]

Mr. Aaron McCrorie: What we did was we outlined the process that we were going through. Very similar to our colleagues in the Correctional Service, we worked with our internal colleagues to assess the need. What we determined was that, rather than doing a PIA for each individual device, what we need to do is do a PIA for the program as a whole, so it's not only how we use those individual devices but how they are being used in the context of the program.

[*Translation*]

Mr. René Villemure: Did you respond to Radio-Canada in the course of its investigation?

Mr. Aaron McCrorie: I'm sorry, but I have to confirm the exact words we used to respond to Radio-Canada.

Mr. René Villemure: Very well.

Mr. Larkin, I'm listening.

D/Commr Bryan Larkin: I would say the same thing. I'm not sure what we said to Radio-Canada, but we will check.

Mr. René Villemure: Very well.

Ms. Gratton, you talked earlier about proportionality when using this tool. Could you tell us more?

Ms. France Gratton: I said we use the tool on seized devices. We've seen a marked increase in the number of incidents involving drones, as well as a significant increase in the number of cellphones seized in facilities.

Accordingly, to collect security intelligence, we use these systems to extract data and prevent other incidents. As for proportional use of this tool, it is indeed necessary to fight contraband and prevent security incidents.

● (1235)

Mr. René Villemure: Would you say it's easier to get information with the help of that tool even if, in the end, it requires authorizations that are just as hard to get?

Ms. France Gratton: No, it's not easier. The information we get this way is compiled with security intelligence we already have. It helps us move the needle in our efforts to prevent contraband materials from getting into our facilities.

Mr. René Villemure: Thank you.

Mr. McCrorie, I have the same question for you: do you use this tool because it's easier? Is the information you get this way more reliable, even if it involves a privacy impact assessment and other processes?

[*English*]

Mr. Aaron McCrorie: I don't think it's a question of more.... If you have a device that's locked with a password, we need the technology to open up that device. That's why, in another era, we would have had a locksmith open a box that would have had receipts in it, for example. Now, when we're dealing with firearms smuggling, we'll have electronic receipts on a cellphone or on a computer. Our only way to access that information is to unlock the device and then translate information on that device into a format that can be used in a court of law.

It's not a question of its being easier. It's the technology we need to use to keep up with the technology that criminals are using.

[*Translation*]

Mr. René Villemure: I see.

Mr. Gagné, I think you have an answer for this question.

Mr. Nicolas Gagné: Mr. Chair, I share Mr. McCrorie's point of view. Technological tools help to get the evidence needed during investigations. It's not a matter of it being easier, it's a matter of getting as much access as possible to evidence.

Mr. René Villemure: Do you use those tools to get around the password that locks the phone or to get the information on the phone?

Mr. Nicolas Gagné: It depends on several factors, like the brand, the model or the types of phone locking mechanisms. Getting around the password is just one of many things the tool allows us to do.

Mr. René Villemure: That's perfect.

Ms. Gratton, at this committee, we're trying to assess different situations in order to propose legislative improvements that would lead to better public policy.

Protecting privacy is a subject that's been on everyone's mind for some time. People are worried. In the various testimonies we've heard at committee, people have told us that when they click "I accept" online, they don't always know what they're accepting. They know they want to get the software, for example, but we are realizing that education on privacy isn't adequate.

Another of the committee's mandates is to maintain public trust in institutions like the Royal Canadian Mounted Police, the Canada Border Services Agency and the Correctional Service of Canada.

Some articles in the media, such as those published by the CBC/Radio-Canada, can sow doubt in the public's mind. As soon as the article in question was published, people turned to me to ask what was going on. They were worried. Do you think you can reinforce the public's trust through this morning's testimony on how you use technological tools?

The Chair: Mr. Villemure, your witness will have to answer very quickly, because your time is up.

Ms. France Gratton: When it comes to trust, it's important to emphasize that these technological tools help us make our facilities safer. Since they're used on contraband cellphones, it means they're used for very specific purposes. The information extracted from cellphones is used only for intelligence purposes. In that way, I think we can show that the tools we are talking about are not used outside of the mandate.

Mr. René Villemure: Very well, thank you very much.

[*English*]

The Chair: Thank you.

Mr. Green, you have six minutes. Go ahead, please.

Mr. Matthew Green: Thank you.

I was sharing with my colleague that I am finding it difficult to imagine that, out of the hundred-plus organizations that I just requested send us back information, we're going to see a huge deviation in the answers that we're receiving.

I think we've established—feel free to correct me if I'm wrong—that the use of this technology is an investigative use, whether it's through law enforcement agencies or through staff in terms of federal employees. I am to understand that most of you have this within the legal framework.

Have any of your agencies used it with your employees?

D/Commr Bryan Larkin: We've used it on one occasion for an internal matter that was on consent, actually. We used digital forensic tools. It was a consent matter.

Mr. Matthew Green: Okay.

Mr. McCrorie.

Mr. Aaron McCrorie: We haven't, to my knowledge.

Mr. Matthew Green: Ms. Gratton.

Ms. France Gratton: No, we haven't used it on employees.

Mr. Matthew Green: Forgive me. I'm not impugning anybody, but drones are one way that contraband comes in. It's sometimes suggested that staff are, on rare occasions, involved in bringing in contraband.

Have you ever had an occasion to investigate or use this technology with any of the corrections staff?

● (1240)

Ms. France Gratton: No. There would be occasions when we would investigate staff. We would not use specific legal software. It would have to be specifically within an investigation.

Mr. Matthew Green: Is it safe to say that all of your staff are issued federally issued devices?

D/Commr Bryan Larkin: A large portion of them are, yes. That would be correct.

Mr. Matthew Green: In your case, none of them are ever monitored in this way.

Mr. Aaron McCrorie: The mandate of my organization is outward-facing. We do criminal investigations involving violations of border-related legislation.

Mr. Matthew Green: That's fair.

Notwithstanding the car thefts, I think we've established the facts, which are that this panel, which I think would have the greatest rationale for and likelihood of using this technology for investigative purposes, has provided very straightforward answers to what this is and what this isn't. I accept that.

We have all these other groups—and I'm just saying this for the purpose of the committee, not as part of the line of questioning. We have at least three or four of these meetings at two hours apiece.

The Chair: We have at least six.

Mr. Matthew Green: I'm going to put on the table right now and say that I'm struggling to find where the conclusion of this will be in terms of the value and the diminishing return on value of the questions.

I'll share with the committee that I am considering a way in which we might be able to digitally communicate with people and share with them a list of agreed-upon questions for response, because I'm not sure how another three days, six hours, eight hours or 10 hours of this is going to go. I know there are lots of people with live motions. I would also state that I'm at a point now in this committee where I'm hoping to steer it back onto our legislative schedule and away from whatever happens to have been in yesterday's headlines, to do the important work of the committee and to hopefully start to address the gaps in legislation.

I just don't know what's left here, so I'm actually done with the rest of my line of questioning.

I thank you all for being here. I don't think there's anything more that needs to be said in terms of the scope of your work. I appreciate you for it. I would say I look forward to seeing you back here again, but that's not always the case.

With that, I'll hand my time back over to the committee.

The Chair: Thank you, Mr. Green. In the two minutes that you would have had left, I'd like to explain where we are right now for the benefit of the committee.

We do have another panel that's scheduled to come in on Thursday. I don't think the notice of meeting has been published at this point, but it will be by later today. Based on the list we had in the motion, the panels will consist of at least three or four of those departments.

The clerk has gathered all of the contact information regarding the motion that was passed the other day about the privacy impact assessments. We haven't done anything with that because we just received the complete list during the meeting. That takes us up to next week, when we're expected to continue with more panels based on the motion. That takes us up to the 27th, when we're going to have the RCMP commissioner and the staff sergeant come in and speak about the SNC-Lavalin motion that was passed as well.

That's where we are right now in terms of the meetings of the committee, Mr. Green.

Go ahead, sir.

Mr. Matthew Green: The one group I'm most keenly interested in hearing from is the unions. I want to hear from the representatives, because if there's no real complaint there from the representatives of the actual federal employees, it becomes very difficult for me to pursue something that may or may not be a privacy issue. I would think that those collective agreements would have stipulated most explicitly where there would be a contravention of their privacy rights.

If it could be possible, Mr. Chair, to prioritize the invitations to our union representatives to come before this committee, for me, that would determine whether this is something I would see fit to continue to pursue.

The Chair: This is a very dynamic meeting. We just received confirmation about Jennifer Carr, who was on the list, from the Professional Institute of the Public Service. She's confirmed for February 15. We may be able to advance. We've had one other confirmation from one of the unions, Mr. Green. We could adapt the meeting schedule to reflect what you said, but have the president of the Professional Institute of the Public Service, Ms. Carr.

We're still in our rounds, but I'm going to open it up for Mr. Barrett for some comments. I will open it up to Ms. Khalid or others if they have other comments as well.

Go ahead, Mr. Barrett.

● (1245)

Mr. Michael Barrett: I'm generally aligned with the thought that we not just have a *Groundhog Day* of meetings, but I do think the question of ministerial accountability is important. These PIAs are not optional, so if we're going to set a work plan to wrap this up before six meetings and Mr. Green wants to prioritize hearing from the workers' representatives, if that box is being checked, then I would say we should prioritize hearing from the people who are accountable for not having gotten the PIAs.

We should prioritize which ministers we want to hear from. I think there was a discussion about having the procurement minister or the Treasury Board minister come before committee, so we should get those on the books. Then Mr. Kurek suggested that, if we had questions for the remaining departments, perhaps we should collect those questions from all parties, set a deadline, submit them to the departments with a deadline for response and then move on.

The Chair: Okay. I appreciate those comments, Mr. Barrett.

As chair I am guided by the clerk and the analysts in following the motion that was adopted by the committee. If there is a desire to take in some of the suggestions that have been proposed during this discussion, then I will need direction from the committee on just what to do in that regard.

Ms. Khalid, Mr. Villemure has ceded to you. Go ahead, please, Ms. Khalid.

I'm just going to ask the witnesses for their patience on this, because we may resume the line of questioning. We don't have much time left.

Ms. Khalid, go ahead.

Ms. Iqra Khalid: Thanks very much, Chair.

I really think the issue that's been highlighted is important. I'm quite intrigued by some of the testimony we've heard thus far. I really agree with Mr. Green that we need to hear from unions and the public service.

Mr. Matthew Green: I'll put that on my campaign poster.

Ms. Iqra Khalid: I really think that, instead of ending it at this time, we should abbreviate it and see if there is something that we as a committee can recommend to ensure that privacy and privacy impact assessments have the value within our departments that they should.

At this time, I am in favour of abbreviating the study with more of a focus on unions and the public service, as Mr. Green has suggested, and going from there.

The Chair: I appreciate the comments. I will tell you that the President of the Treasury Board has been invited. We're waiting for a date for that.

What I'm hearing are two sides. There is what Mr. Green has suggested, and then there is what Mr. Barrett has suggested. Mr. Green wants to hear from those who are impacted. Mr. Barrett wants to hear from those who are in charge. Perhaps the clerk and the analysts and I can collectively find a way to get to that point over the course of the next couple of meetings. The challenge we have is that we do have the meeting ready to go on Thursday, and it will involve departments as per the motion. We can continue on with that. We may abbreviate the number of meetings down from six to maybe five at this point, because this is the second one that we've had on this.

Mr. Green, I saw your hand. Go ahead, please.

Mr. Matthew Green: We can negotiate in public with the Treasury Board president and the staff who are watching to say that, if they can be available to this committee sooner rather than later, then we can wrap it up. Otherwise, we're going to be in a scenario of having all departments come before the committee. Let's hopefully get that as a bit of an incentive for the president to come before the committee.

● (1250)

The Chair: Here's what I would like to do then.

Mr. Green, if possible, we can continue for the next few minutes with our witnesses. I'm going to suggest that we continue with the next meeting with the departments. We will have a committee business meeting, at which I can update the committee on where we are with the witnesses. We've taken about 10 or 15 minutes on this, which I think is unfair to the witnesses who presented themselves today.

I think we have clear direction from the committee on where we want to go with this. I would ask now that we continue with our witnesses. We'll go ahead with Thursday's meeting and then have a subcommittee meeting at that point. I'll make time for that if that's okay. Then I can update you on where the President of the Treasury Board is and where some of the other witnesses that were suggested here in this discussion are. Is that fair? Are we agreed? Okay.

We have Mr. Green's round completed.

I think I have Mr. Kurek next for five minutes.

Go ahead.

We're going to have very shortened rounds here. We do have a little bit of extra time because of the suspension, but we'll have five, five, two and a half, two and a half, and then we'll conclude.

Go ahead, Mr. Kurek.

Mr. Damien Kurek: Thanks very much.

I appreciate the witnesses.

I will just give some unsolicited advice. Let's be proactive on PIAs. The commissioner came before the committee and said that he wants to work with you and that he will be as responsive as he possibly can, so let's make sure—instead of our finding out from the media and going through this rigamarole—that departments, agencies and the like are proactive. I think that will save you all a lot of these tough questions.

We had different witnesses in the first hour of this meeting who talked a lot about the potential use of this technology when it comes to employees. I know there are ECCC, NRCan and a whole host of others. You're talking about this in terms of law enforcement and its application, but I just want to, if I may, find out where you are in terms of the people who work for your departments—those within law enforcement administration. I do not mean the program specifically, because you have answered on that very clearly, but I'd like to hear from you about whether there are tools, techniques and methods through which you would observe employees and other individuals who work for you in terms of the data that could be on their devices.

Let's start with the RCMP. I'm hoping for very brief responses, because I have some other questions.

D/Commr Bryan Larkin: Thank you for the question.

In short, no, we do not use any technology to monitor and/or manage or supervise our employees. We do have a user agreement for all of the devices we deploy. We do have a policy that governs the use of those devices.

Naturally, within our organization sometimes members are subject to allegations regarding code of conduct and/or criminal obligations, and we may need to launch an internal investigation, part of which may be to look at using digital forensic tools. As I alluded to, we've used them on one occasion with consent.

Mr. Damien Kurek: I apologize, but I'm really short on time.

Mr. McCrorie, go ahead.

Mr. Aaron McCrorie: Again, professional standards investigations take place outside of my particular organization, so it's hard for me to comment on their techniques and what they do.

Mr. Damien Kurek: I would ask you to bring that up to whoever within the CBSA is responsible for that and to ask them to provide that answer in writing to this committee. That would be very helpful.

Ms. Gratton, go ahead.

Ms. France Gratton: I would say the same thing. We don't use any tools to observe or monitor our staff. That's like the same situation—

Mr. Damien Kurek: Again I would ask that you bring that up the chain and make sure to get those answers to the committee.

Mr. McCrorie, I am curious, because there has been talk about investigations. Over the course of COVID there were conversations around ArriveCAN and a whole host of instances surrounding that and about people who crossed the border during the pandemic when there were restrictions. Were these sorts of investigations ever initiated because of COVID-related enforcement?

Mr. Aaron McCrorie: What we're doing is enforcing criminal elements of border-related legislation, for example, with respect to individuals who have been counselling others on how to fraudulently obtain immigration documents, a student visa or a work visa, or individuals who have been involved in the smuggling of firearms or parts. There was a case that went to court last year, in April 2023, and the individual got roughly 12 years for manufacturing ghost guns and for smuggling the parts in. Those were the instances in which we used those tools to get the evidence, as did our colleagues in the RCMP, to successfully prosecute those who had broken the criminal laws.

Mr. Damien Kurek: It's very clearly limited to breaches of the Criminal Code, so for somebody who—

● (1255)

Mr. Aaron McCrorie: It was border-related legislation, so they were booked, for example, under our own Customs Act.

Mr. Damien Kurek: Okay. You're telling me—and feel free to clarify—that when it came to any COVID-related enforcement, this technology would not have been used.

Mr. Aaron McCrorie: I'm not aware of any instance and I can't think of an instance in which we would use it in the context of COVID. Again, the only instances in which we would use it would be with prior judicial authorization.

Mr. Damien Kurek: I appreciate that.

Ms. Gratton, I have just a few seconds left here. There are, for example, safe injection sites in our prisons, but it's kind of “don't ask, don't tell” when an inmate goes to a safe injection site to use contraband. Quite often they have had to get that from somewhere. I'm just trying to square this circle here about enforcement and whatnot when it comes to the dynamics in a prison, where there's alleged criminal activity but it's “look the other way” when it comes to certain aspects of that.

Could you comment briefly on how I square that?

The Chair: Boy, does it ever have to be brief.

[*Translation*]

Ms. Gratton, I’m sorry, but you will have to answer quickly.

[*English*]

Ms. France Gratton: Just quickly on overdose prevention sites, it's not a question of not looking at it. It's a harm reduction program, and it's really to enforce support and help inmates who are struggling with substance use. The distinction is that, when we are dealing with trafficking, then we go with the enforcement. That's where we get into taking measures and discipline to prevent the trafficking and the contraband. It's two different approaches.

The Chair: Thank you, Ms. Gratton.

Thank you, Mr. Kurek.

Mr. Housefather, you're next. You can have unlimited time—

Voices: Oh, oh!

The Chair: —since you're a new guest to the committee.

Mr. Anthony Housefather (Mount Royal, Lib.): Thank you, Mr. Chair. That was very flattering.

In order to save time, I just want to clean up on some issues. I'm going to ask my questions of the RCMP, and I'm going to ask the other departments to affirm if the answers the RCMP give me are the same as they would also have.

The first thing is the confusion among spyware, malware and data extraction technology. Spyware and malware are bad things that people put on your phone to continuously extract data and use it for nefarious purposes.

For the RCMP, can we assume that we don't use spyware or malware whatsoever and that we simply use data extraction tools?

[*Translation*]

Mr. Nicolas Gagné: No, not at all.

[*English*]

Mr. Anthony Housefather: Is it the same?

[*Translation*]

Mr. Aaron McCrorie: Same thing for us.

[*English*]

Mr. Anthony Housefather: It's the same also. That would mean that, when you extract data, you've taken the device, you've extracted the data and you do not leave anything on the phone or the tool that you extracted the data from. Is that correct? You would give it back without leaving any type of software on it to continue to extract.

Mr. Nicolas Gagné: That's correct.

Mr. Anthony Housefather: Is it the same?

Mr. Aaron McCrorie: I'd say it varies by the circumstances. Remember that this is evidence in a criminal procedure, so we will hold that as part of our evidence and for part of it we use the tools to extract and translate the data into a format that can be used in judicial—

Mr. Anthony Housefather: No, I understand, but you're not giving someone back the phone with a tool on it to continue to extract their data without their knowledge.

Mr. Aaron McCrorie: No.

Mr. Anthony Housefather: Is the same true, Ms. Gratton?

Ms. France Gratton: We are not giving back the phones because they are contraband, so we keep them.

Mr. Anthony Housefather: I understand.

Would it be true, in the case of the RCMP, that you are using technology to extract data that is consistent with RCMP-type organizations in the United States, in the U.K. and in other similar types of countries?

Mr. Nicolas Gagné: I would say so, yes.

Mr. Anthony Housefather: Would you say that the policies that you use are consistent as well, noting the difference in our criminal law?

Mr. Nicolas Gagné: I would say they're somewhat similar, yes.

Mr. Anthony Housefather: Thank you.

Would you say that as well for the CBSA?

Mr. Aaron McCrorie: To the best of my knowledge, yes, and I would say it's also very similar to how our colleagues use it.

[*Translation*]

Mr. Anthony Housefather: Is it the same thing for the Correctional Service of Canada?

[*English*]

Ms. France Gratton: I would say there are some differences depending on the jurisdiction, but it can be similar, yes.

Mr. Anthony Housefather: Perfect.

I would now want to just establish that these devices that you have cannot be used remotely. In order to use the data extraction technology, you actually need to have the device in hand. Is that right? You cannot surreptitiously take data off a device that is not in your possession and the user have no knowledge that you're doing that. Would that be correct?

Mr. Nicolas Gagné: For the technology in question here, the Cellebrites or the Magnet Forensics of this world, yes. We need the device in our hands to extract the data.

Mr. Anthony Housefather: A Canadian sitting in Winnipeg can be sure that the RCMP is not, never having had possession of their device, extracting data from it.

Mr. Nicolas Gagné: Using these tools, that's correct, yes.

● (1300)

Mr. Anthony Housefather: We won't get into what other tools you may have at this point, because that would be another study.

CBSA...?

Mr. Aaron McCrorie: Yes, we use the technology in our digital forensics labs, secure facilities. It's in our physical possession, again, obtained through a search warrant.

[*Translation*]

Mr. Anthony Housefather: Perfect.

Is it the same thing for you, Ms. Gratton?

[*English*]

Ms. France Gratton: It's exactly the same, yes.

Mr. Anthony Housefather: I have one last question.

You mentioned the one time only that you used this on an employee. My understanding, then, is that, if you're ever using it on an employee, it's a result of potential criminal activities by that employee. It's not because they're breaking HR protocols of the RCMP that don't get into criminal law, other than in that one instance. Is that correct?

D/Commr Bryan Larkin: This one was actually not a criminal investigation. It was an internal matter. It was a departmental security investigation, and the member actually consented. They came forward and consented to use the device on their tool.

Mr. Anthony Housefather: They did so in order to clear themselves, I presume. They felt that the information there would clear them.

What I'm asking, then, is that, just like any other potential criminal activity that exists, I would assume, if the criminal activity exists with an employee of the RCMP, then it would fall under the warrant provisions and the other provisions that you use with anybody else. You wouldn't be dealing with the employee for employee matters, except, as you mentioned, through consent to do that.

D/Commr Bryan Larkin: For a criminal investigation, we would seek judicial authorization, although there are authorities under the RCMP Act that would allow us to actually use the technology, use the actual tools, but we would use that on a case-by-case basis. Superintendent Gagné's team looks at a threshold and a framework, and there's consultation with our professional responsibility office and the investigators doing that code of conduct investigation.

Mr. Anthony Housefather: It's done knowingly. Employees are already signing on to policies that are well in their possession. They know this.

D/Commr Bryan Larkin: That is correct.

Mr. Anthony Housefather: Is it the same thing?

Ms. France Gratton: Yes.

Mr. Anthony Housefather: Thank you very much, Mr. Chair.

The Chair: Thank you, Mr. Housefather.

That concludes our panel for the second hour.

Monsieur Gagné, Mr. Larkin, Mr. McCrorie, Madame Gratton and Mr. Matson, thank you so much for appearing before the committee today.

For the sake of the committee, we have scheduled Environment and Climate Change, Fisheries and Oceans, the CRTC and the Canada Revenue Agency for Thursday. We're taking the advice of the committee. We're trying to get who we need to get before this committee sooner rather than later in order to continue this study.

I want to thank the clerk, the analysts and the technicians for today's meeting.

The meeting is adjourned.