HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

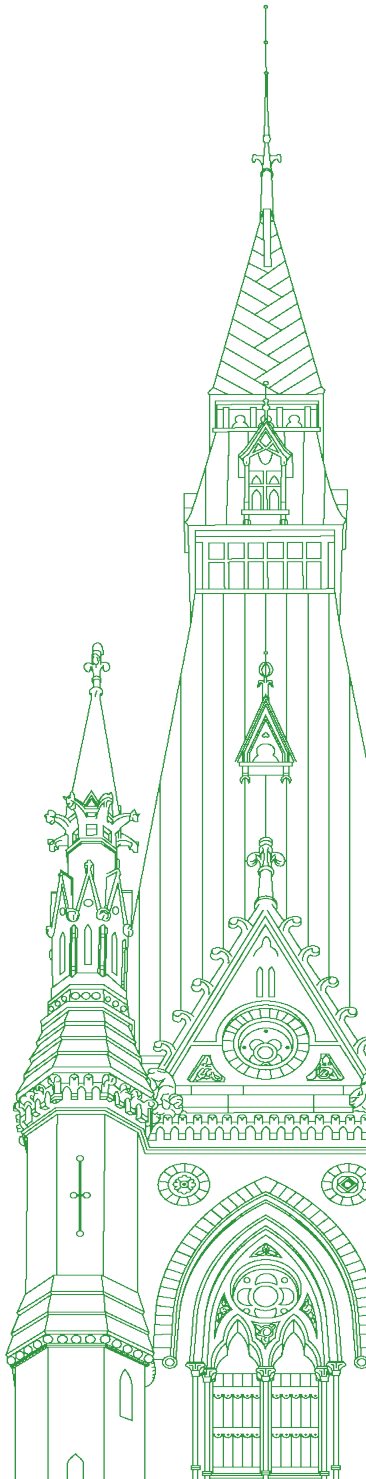
44th PARLIAMENT, 1st SESSION

Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 102

Thursday, February 8, 2024



Chair: Mr. John Brassard

Standing Committee on Access to Information, Privacy and Ethics

Thursday, February 8, 2024

● (1105)

[*English*]

The Chair (Mr. John Brassard (Barrie—Innisfil, CPC)): Good morning, everyone. I call the meeting to order.

[*Translation*]

Welcome to meeting No. 102 of the House of Commons Standing Committee on Access to Information, Privacy and Ethics.

[*English*]

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

[*Translation*]

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 all members—I know that the witnesses have been briefed on this—to be mindful of the earpieces. If they're too close to the microphones, they could cause hearing damage to our interpreters.

I would now like to welcome our witnesses for the first hour. From the Department of Fisheries and Oceans, we have Brent Napier, acting director general, conservation and protection; and Sam Ryan, director general, integrated technical services. From the Department of the Environment, we have Hannah Rogers, director general, environmental enforcement; and Donald Walker, chief enforcement officer.

I'll start with the Department of Fisheries and Oceans. You have up to five minutes to address the committee.

Please go ahead.

Mr. Brent Napier (Acting Director General, Conservation and Protection, Department of Fisheries and Oceans): Hello and good morning, Mr. Chair and committee members.

My name is Brent Napier. I am the acting director general of the conservation and protection directorate at Fisheries and Oceans Canada. I am joined today by my colleague Sam Ryan, director general of DFO IT operations.

Before I begin, I would like to acknowledge that I am grateful to be joining you here on the traditional, unceded territory of the Anishinabe Algonquin people.

Mr. Ryan and I appreciate the opportunity to appear before this committee on behalf of Fisheries and Oceans Canada and provide you with information on the conservation and protection program and our national digital forensics service, which fall under my responsibility, and the cybersecurity digital forensic investigator service, which is under Mr. Ryan's responsibility.

[*Translation*]

It is the enforcement program of Fisheries and Oceans Canada. The Department's mandate is to sustainably manage fisheries and aquaculture. The proper management of fisheries and marine and aquatic resources requires a robust compliance verification program.

[*English*]

C and P has over 550 fishery officers in locations across Canada. Our officers work with the general public, harvesters, indigenous communities and industry to conserve and protect Canada's marine and aquatic resources. Fishery officers verify compliance with fisheries-related statutes, such as the Fisheries Act and the Species at Risk Act, and take enforcement actions, including undertaking investigations and recommending prosecution for offences.

Historically, the harvesting and reporting of fisheries resources was all done using paper forms, such as logbooks and charts. As technology has advanced, harvesters have adopted new technology, such as chart plotters, electronic logs and electronic communication devices into their harvesting operations. To remain an effective enforcement organization, C and P has adapted its capacity, tools and use of technology. This includes the implementation of new units to support complex investigations, including those involving complex digital files, components and data. Digital forensics examiners are now part of the C and P team. They use new digital technologies, technological solutions and approaches to support digital enforcement investigations.

C and P's digital forensics team is centrally managed in Ontario and supports fishery officers across the country through regional labs. The digital forensics team is made up of seven experienced, highly trained and highly skilled digital forensics examiners. The training and technical solutions used by the C and P digital forensics team is in line with Canadian municipal, provincial and federal law enforcement standards. Before deploying any technical solution or retrieving any digital data, C and P's fishery officers and investigators seek a judicial authorization or warrant.

The IT operations' cybersecurity digital forensic investigator team uses digital forensics tools to support the department's mandate to promote and maintain compliance with legislation and regulations as well as internal administrative investigations into violations of Government of Canada policies, such as fraud or harassment in the workplace, and for supporting such cybersecurity activities as investigating cybersecurity incidents.

In the context of an administrative investigation, it is important to note that judicial authorization is not required. It is conducted with the full awareness and co-operation of the involved individual. The nature of the allegations and the subsequent investigation are defined within the investigation's terms of reference, which are shared with the involved individual.

In closing, the Government of Canada, including Fisheries and Oceans Canada, is committed to working with other federal departments and agencies, provincial and territorial governments, indigenous peoples and other partners to fulfill its commitment to protect, enhance and restore the biodiversity and health of Canada's marine and freshwater environments through an integrated ecosystem approach that supports the sustainable use of marine and aquatic resources.

Thank you for your attention. I will be happy to answer any questions you may have.

The Chair: Thank you, Mr. Napier.

Next, we're going to the Department of the Environment. You have up to five minutes.

Mr. Walker, I assume you're going to start. You have five minutes, sir, to address the committee. Go ahead.

Mr. Donald Walker (Chief Enforcement Officer, Department of the Environment): Good morning, members of the committee. It is a pleasure to be here with you today.

My name is Donald Walker, and I am the chief enforcement officer at Environment and Climate Change Canada. I'm joined by my colleague Hannah Rogers, who is the director general of environmental enforcement.

[*Translation*]

We are pleased to be here to explain our mandate and provide you with an overview of our operations. I will also talk about our use of digital forensics software.

[*English*]

Environment and Climate Change Canada administers several environmental statutes and their associated regulations. These include the Canadian Environmental Protection Act, the pollution prevention provisions of the Fisheries Act, and the Greenhouse Gas Pollution Pricing Act, among others. We also enforce wildlife laws, such as the Wild Animal and Plant Protection and Regulation of International and Interprovincial Trade Act, the Migratory Birds Convention Act and the Species at Risk Act.

The Environment and Climate Change Canada enforcement branch was formed in 2005 with a mandate to conduct inspections to verify compliance with these laws and their associated regulations, investigate possible violations and take action to compel compliance when violations are identified.

[*Translation*]

With nearly 500 employees across Canada, the Environment and Climate Change Canada enforcement branch is comprised of uniformed enforcement officers who have the powers and protections of peace officers when enforcing the laws under which they are designated. These officers conduct thousands of inspections per year to verify compliance.

● (1110)

[*English*]

If enforcement officers find sufficient evidence of an alleged violation under the environment and wildlife protection acts for which they are responsible, they will take appropriate action in accordance with our compliance and enforcement policy. These actions are designed to restore compliance and may include issuing warnings, directions, compliance orders, tickets and administrative monetary penalties. When the environmental harm or the factual circumstances warrant it, officers conduct investigations and collect evidence to support the laying of charges.

[*Translation*]

To this end, Environment and Climate Change Canada's enforcement branch works closely with colleagues at the Department of Justice Canada and the Public Prosecution Service of Canada to build prosecutable cases.

[*English*]

Since the creation of the enforcement branch, the nature of the non-compliance we uncover has changed and the evidentiary requirements to establish non-compliance in court have grown more complex.

While the majority of our regulated sectors are compliant, we also respond to non-compliance by organizations and individuals who sometimes go to great lengths to conceal or hide the negligence that led to serious environmental damage or biodiversity loss. This has only increased as the courts have issued more serious penalties.

In response to this changing reality, enforcement received a mandate in 2020 to modernize its operations. This included the implementation of a risk-based approach for setting its inspection priorities to ensure that its resources are targeted where the potential for environmental damage or impact on wildlife is greatest. It also included investments in new information technology infrastructure, data analytics capacity and digital forensics software, in large part to ensure that we could meet modern information management expectations as well as provide evidence to meet the standard of the courts.

Our digital forensics lab is staffed by a small number of specialized analysts. These employees are highly trained professionals, who are trained first as enforcement officers and then as digital forensics experts. This training ensures that they understand the limits of their authorities and the specific mandate of the digital forensics unit.

The digital forensics software we use can only be employed under warrant, and only within the context of enforcing Environment and Climate Change Canada legislation. Digital data that can be imaged or acquired are extracted on site during the execution of a court order. Devices from which data cannot be extracted on site are collected and brought to the national laboratory. Digital evidence that is collected typically consists of information that can be stored on smart phones, laptops, cloud-based storage systems, servers and flash drives.

[*Translation*]

Digital forensics analysts are the only people within Environment and Climate Change Canada who use such tools. Our department must continue to evolve and innovate to remain effective, but these new tools require that we continue to pay close attention to how we manage information, particularly as it relates to privacy.

[*English*]

Environment and Climate Change Canada takes privacy very seriously and to this end enforced a comprehensive review of its information management procedures, including for the use of digital forensics software. We are completing new privacy impact assessments, with those that focus on our operational activities being prioritized. We communicated our intentions to the Privacy Commissioner in June 2022.

This review, which started in 2023, will include specific tools like digital forensics software. The operational components are our priority. The privacy impact assessment that covers forensics software will be completed in the upcoming fiscal year.

Thank you for your attention. I will be happy to answer questions from the committee.

The Chair: Thank you, Mr. Walker.

First of all, I want to welcome the members of the committee who are here today. We have an all-star cast.

Mrs. Kusie, Mr. Oliphant, Mr. Housefather and Ms. Idlout, welcome to the committee.

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

[*Translation*]

Mrs. Stephanie Kusie (Calgary Midnapore, CPC): Thank you very much.

[*English*]

Mr. Chair, it's always a pleasure to be here at the ethics committee, the ethical heartbeat of Parliament, since the Prime Minister doesn't have one.

I'd like, first of all, to thank my colleagues for their good work with the Privacy Commissioner, Philippe Dufresne, who said he first learned of these tools being used by at least 13 federal departments and agencies through a Radio-Canada report published in November—shocking. He also stated that his office should not be learning about the use of such technology after the fact, which I think is a very important piece of information, despite the fact that in appendix B of the directive on privacy impact assessment, it states:

> Government institutions seeking Treasury Board approval for—

Of course, Mr. Chair, I do fundamentally hold the President of the Treasury Board responsible for this incredible lapse. It continues:

> —activities that involve personal information are responsible for:
>
> Making every reasonable effort to initiate the PIA at the earliest possible phase of project planning; [and]
>
> ...identifying the timelines for the completion of the PIA....

However, the Privacy Commissioner told this group, my colleagues, that he learned about this after the fact.

Mr. Ryan, did your department procure surveillance gear that can be used to access employees' information and potentially the information of Canadians at large—yes or no?

● (1115)

Mr. Sam Ryan (Director General, Information Technology Operations, Department of Fisheries and Oceans): Thank you very much for your question.

We do not have surveillance equipment. I think you asked about surveillance gear. We do not have surveillance equipment. The actual software that we have is used as part of our administrative investigations, and it's used with the full understanding of the employees involved. It follows a very rigorous process where we go through a terms of reference that is shared with the individuals, and they're fully aware about what is within and not within the scope.

Again, it's not surveillance, because we actually have to have the equipment. Whether it's a laptop in question or a government-issued phone in question, they have to be within our forensics unit.

Mrs. Stephanie Kusie: Okay.

Was this software procured without the use of the privacy impact assessment?

Mr. Sam Ryan: I believe the software in question is one of our forensic tools. Again, like all software, it goes through many different iterations of the tool. I think that tool has been sold for many years, potentially more than 10 or 15 years. I believe it started to be used when it wasn't possible to actually copy your contact details from your flip phone. I believe that's how this software came into being.

Again, it's more than, I think, 15 or 20 years that these forensic tools have been in place, and I believe the PIA came into force in 2010 approximately.

Mrs. Stephanie Kusie: Okay, but is a PIA required for these tools?

Mr. Sam Ryan: Again, a PIA, as I understand it, is part of the overall process or program that's being evaluated. When we're looking at it, again from my perspective, it is administrative investigations, so that process or that program has been in place for many decades. The tool that we're talking about—

Mrs. Stephanie Kusie: Was it required for the tools, the PIA? Is it required for this software?

Mr. Sam Ryan: Again, the PIA is not software-specific. It is for the program. The tool is one part of the program.

Mrs. Stephanie Kusie: Okay. I will take that as a yes.

Did you receive any direction from the Treasury Board when it was announced that your department had not filled out the required PIAs?

Mr. Sam Ryan: I, personally, was not a part of those communications. I know within our department the ATIP office was in communication, I believe, both with the Privacy Commissioner and with Treasury Board. That is the mechanism by which the communication happens within our department, the central agency and the Privacy Commissioner.

Mrs. Stephanie Kusie: Okay.

Have you received any indication from the President of the Treasury Board on enforcing compliance with this important requirement for the PIA? Have you received any direction from the Treasury Board specifically?

Mr. Sam Ryan: Again, from my perspective, all those communications would happen between our ATIP office, the Treasury Board and the Privacy Commissioner. Those communications have happened, I believe, but I'm not personally privy to the specific communications.

Mrs. Stephanie Kusie: Mr. Walker, do you have the same software, or has your department procured surveillance gear similar to that of Mr. Ryan or otherwise, to access employees' information and potentially the information of Canadians at large?

Mr. Donald Walker: We have acquired the same software about which we are speaking today.

It is not intended for ongoing surveillance of Canadians. We do not, in Environment and Climate Change Canada, use the software for employee devices.

Mrs. Stephanie Kusie: What is your justification for procuring this software without the use of a privacy impact assessment?

Mr. Donald Walker: I will turn shortly to my colleague, Ms. Rogers, to talk a little bit about the protections we have in place.

At the time that the digital forensics unit was established in 2013, this was viewed as a natural evolution of the search warrant process, where we seek court orders to acquire specific information.

Certainly, we would not expect that the enforcement branch of Environment and Climate Change Canada would not access information unless it had been printed for the purposes of pursuing noncompliance under environmental or wildlife protection legislation.

I would ask Ms. Rogers to speak briefly about the protections in place.

● (1120)

Mrs. Stephanie Kusie: That's fine, Mr. Walker.

Can you be clear as to whether you received any direction from the Treasury Board when it was announced that the required PIAs were not filled out for this type of software?

Mr. Donald Walker: Like my colleague, I cannot say definitively whether the department received specific information from the Treasury Board, but Environment and Climate Change Canada already had a privacy impact assessment development process under way at the time of the reporting on this last year.

Mrs. Stephanie Kusie: Thank you, Chair.

The Chair: Thank you, Mrs. Kusie.

Next, we're going to Ms. Khalid.

Go ahead for six minutes, please.

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

Thank you to the witnesses for appearing today.

To follow up, Mr. Walker, when did you acquire these technologies?

Mr. Donald Walker: My understanding, and I will turn to my colleague for confirmation, is that it was in 2013 as part of the creation of the digital forensics—at the time computer forensics—program in the enforcement branch of the ECCC.

Ms. Iqra Khalid: That's interesting. Maybe we should ask the previous Treasury Board to come in to answer some of these questions.

I've been asking questions...and I will turn to each of you, one by one.

What, in your opinion, is the importance of having a privacy impact assessment?

Mr. Donald Walker: From an Environment and Climate Change Canada perspective—and I will turn to my colleague again to provide further details—the importance is to make sure that we have the rigours in place to ensure the proportionality of the tools we're using and that we have appropriate measures in place to protect the information.

Ms. Rogers.

Ms. Hannah Rogers (Director General, Environmental Enforcement, Department of the Environment): Yes, I'd add that we have a number of safeguards in place. The information that is gathered using these tools is only accessed by highly trained officers in very few numbers.

Ms. Iqra Khalid: My apologies. My question was what the importance is, in your opinion, of having a privacy impact assessment.

Ms. Hannah Rogers: We take the privacy of all Canadians very seriously.

As Mr. Walker mentioned, we have a PIA under way at the moment and we will continue to complete that work. We expect the PIA that relates to our operational activities to be completed in this next coming year.

Ms. Iqra Khalid: Why did we not do a PIA when it was required?

Mr. Donald Walker: At the time of the development of the program, it was viewed as a natural extension, and there was not an intent to collect personal information.

As Ms. Rogers mentioned, we have a specialized team that works on the computer forensics itself, which is separated entirely from the investigators on the file, so there is a wall in between the two pieces of information. The digital forensics experts are trained to seek out the exact information that is being sought under the court order and to disregard any personal information that is being collected.

At the time, and this would precede both of us, the understanding was that, because this was not intended to collect or store personal information, it might not have been required. We have since, out of an abundance of caution and starting in 2022, determined that with the modernization of our activities in the Environment and Climate Change Canada enforcement branch, there is value in conducting privacy impact assessments across the range of our activities.

Ms. Iqra Khalid: Thanks very much.

Are you surveilling Canadians at large?

Mr. Donald Walker: We are not surveilling Canadians at large. There are occasions, as with any operational law enforcement organization, when we will monitor certain sites where we expect non-compliance to occur. For instance, in the case of the Migratory Birds Convention Act and the regulations that are associated with this, if someone has laid bait in a hunting zone within the 14 days prior to a hunting season's beginning, it's important for our officers, when a physical presence may serve as a deterrent, to observe more discreetly in order to determine who is engaged in non-compliant activity.

Ms. Iqra Khalid: Thanks very much.

Turning to Mr. Ryan and Mr. Napier, I have the same question.

What's your opinion of the importance of a privacy impact assessment?

Mr. Brent Napier: Perhaps I can start. It's to manage risk, to inform operations in process and to, of course, protect privacy above all.

Ms. Iqra Khalid: Why did you not fulfill the PIA requirements when they were necessary?

Mr. Brent Napier: Much like my colleagues from ECCC, these are legacy programs that predate many of our current rules and policies. They were seen as an extension of what we had conducted in the past. In fact, these tools are more surgical in the sense that they can direct us to the files we're looking for instead of having to comb through paper files, where you would basically be privy to information you wouldn't otherwise need.

● (1125)

Ms. Iqra Khalid: Are you surveilling Canadians at large?

Mr. Brent Napier: We absolutely are in the fishery but not with these tools.

Ms. Iqra Khalid: Can you expand on that a little bit? What does that mean?

Mr. Brent Napier: Fishery and Ocean fishery officers, some 550 of them, are on the water and conducting surveillance of the activities that are occurring there through more traditional means of patrols and inspections, but these tools are not part of that tool box for them.

Ms. Iqra Khalid: I'm talking specifically about the digital forensic technologies we're talking about.

Are you surveilling Canadians through this technology, sir?

Mr. Brent Napier: We absolutely are not.

Ms. Iqra Khalid: That's good to hear.

Are there instances when you do need to use these tools? Obviously, you've acquired them. What are those instances?

Mr. Brent Napier: For us, it's all in relation to verifying compliance under warrant. For us, when moving from inspection to investigation, we use these tools to collect evidence and follow the evidentiary process. We use judicial authority with a warrant, where the warrant provides strict guidance and direction on the types of information we have access to and that governs our process and the use of these tools.

Ms. Iqra Khalid: Are individuals aware that these forensic tools are being used for that?

Mr. Brent Napier: They absolutely are, because they have been served the warrant.

Ms. Iqra Khalid: Where do you store this information?

Mr. Brent Napier: We benefit from having three labs that are especially designed to encase evidence, so they're air-gapped and secure. All information, including information that might be collected in the evidentiary collection process and private information that might not directly be relevant, is housed in this area as well. It's not in the cloud. It's not on the network, and it's well protected. There is limited access to these facilities with 24-hour surveillance, and only the examiners use it with fishery officer guidance.

The Chair: Thank you, Ms. Khalid and Mr. Napier.

[*Translation*]

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

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

I'd like to thank everyone for being here this morning. It will give us an opportunity to examine the subject in greater depth. On the basis of what I heard earlier, I must say that it seems to be more of an exercise in obfuscation.

Mr. Walker, your concern for privacy strikes me as insubstantial at best. Could you please give us further details?

Mr. Donald Walker: We take privacy very seriously. I'll explain the problem we encountered.

When the program was introduced, we believed the existing measures were adequate to counter any privacy concerns stemming from our work. However, in view of the changing overall pattern of our work, we decided that the time had come for a complete review of these measures, with additional precautions to ensure that there was a proper framework for them and that they would include a privacy impact assessment.

Mr. René Villemure: So there was an ongoing operation at the department. At some point, you acquired tools of this kind with a view to determining how you might be able to use them. Later, the Treasury Board report advised you that privacy impact assessment was needed. However, it does not appear to have been done.

In fact, a CBC story reported that some departments, including yours, had not done a privacy impact assessment or had not responded to questions in connection with the story.

You didn't mention that you were doing an assessment of this kind. According to the CBC story, none were done.

Mr. Donald Walker: You may be right. I can't remember exactly how we responded in connection with this story.

It was probably the third time in two years that the media had asked us questions like that, and information about obtaining this type of software is publicly accessible on the Internet. In each instance, I don't think we attempted to hide the fact that we were using tools like these in fulfilment of our mandate. On the other hand, I can't recall whether or not we had told the journalists that we were about to undertake an assessment.

● (1130)

Mr. René Villemure: According to the stories we know about, the answer was no. That may not have been correct, but the answer was no.

You've been caught out on that one.

Mr. Donald Walker: By the story?

Mr. René Villemure: Yes.

Mr. Donald Walker: No. We sometimes field questions from the media about the use of various tools, including the software we've been discussing today. As I mentioned, that was the second time we received a request of that kind in 2023. I believe the first came from the *Journal de Montréal*.

Mr. René Villemure: When people from the Royal Canadian Mounted Police or the Canadian Security Intelligence Service appear before the committee, we take surveillance tools for granted. It's expected. When people from the Department of Fisheries and Oceans or the Department of the Environment appear together, it's assumed that you're monitoring trees or the ocean.

There are no doubt good reasons for doing this, but I'd like to hear what you have to say about it. Is it proportionate to the risk you are attempting to mitigate?

Mr. Donald Walker: Definitely. Not only that, but I will refrain from using the term "surveillance", because that's not at all what we're doing with this software. It's used to collect data from electronic devices. It's like opening a drawer while executing a search warrant. We only do it when there's a warrant.

Mr. René Villemure: What precisely are you looking for? I'm curious.

Mr. Donald Walker: It depends on the subject. My colleague's expertise might be helpful to you.

Ms. Hannah Rogers: By all means.

When we look at the data, we're only looking for information we would like to find in connection with the investigation process. So if we look at what is…

Mr. René Villemure: I'm going to interrupt you briefly. You're looking for what you're trying to find so that you can find what you're looking for. That makes sense. But you are with the environment department. You're not looking for bandits.

[*English*]

Ms. Hannah Rogers: For example, we apply the laws that relate to environmental protection and wildlife. For example, if a mining company has committed an infraction under the Fisheries Act, we will be looking for any evidence they have that shows they knew they were conducting such an event that might cause a spill, or for what kind of technical information they have that might be relevant to the investigation.

[*Translation*]

Mr. René Villemure: This tool makes me think of a bazooka. Is the means proportionate to the suspected offence?

Ms. Hannah Rogers: I definitely believe so. We can't obtain the information without these tools. For example, if we have a computer…

Mr. René Villemure: Are there no alternatives to extracting this data?

Ms. Hannah Rogers: None that we could use if we want to continue the investigation.

Mr. René Villemure: What was previously done over the past 50 years before the tool existed?

Ms. Hannah Rogers: We had paper. There were no electronic devices.

Mr. René Villemure: Okay. So it's the introduction of the electronic devices that changed everything.

Thank you very much.

The Chair: Thank you Mr. Villemure, Ms. Rogers and Mr. Walker.

[*English*]

Ms. Idlout, you have six minutes. Go ahead, please.

Ms. Lori Idlout (Nunavut, NDP): *Qujannamiik.Uplaakut.*

Thank you, Mr. Chair.

I am honoured to sit here at the moment to replace my colleague Matthew Green. I'm finding this study quite interesting. It's an area that I wasn't really interested in, but I'm finding the responses fascinating.

To both agencies, based on some of the responses to questions raised by the Liberals about the use of the PIAs, can you confirm whether you had to use them and at which point?

I'll start with Donald.

Mr. Donald Walker: Our understanding of the program is that, when it was first inaugurated in 2013, the view at the time was that the protections in place to avoid the collection of personal information and simply focus on the evidence of non-compliance under a court order would not, under the decision tree, necessitate a privacy impact assessment. However, in 2020, as we were going through a modernization exercise with respect to implementing a risk-based approach to our enforcement activities and a periodic review of our directives, we felt that it was prudent to engage in new privacy impact assessments to cover not just a specific tool but also the activities we undertake so that it takes into account the context in which different tools are used.

● (1135)

Mr. Brent Napier: To echo much of what was said, the other part for us is that there's reasonable belief that an offence has been created. It's not simply during an inspection or just to comb the area. We have a situation where we have reason to believe that an offence has been created. Now we're into the investigation stage of it, where we bring in a judicial authority. It's very clear at that stage. We have to present our case and we have a judge who says, yes, this is the type of information we're allowed to take and what is reasonable. At that stage, we execute.

In terms of your question on a PIA, again, the mechanics on evidence collection have not changed; the tools have. For our purposes, we're not focused on the tool. We're focused on the process. I think it is warranted at this stage to review those processes to ensure that we are protecting privacy. We feel that there are safeguards, significant safeguards, in place, but we have, ourselves, voluntarily agreed to go ahead with the PIA process. We have, ourselves, engaged with the Privacy Commissioner in December. We are executing that process as well, but on the process and not the tools.

The tools will change over time. They come out with new versions and new tools, and all of these tools are not the same. Some are designed to allow access to cellphones and technology. Others search deleted items and allow us to recover those files. There's a series of different tools for each of the different jobs, but again, they're strictly defined by a court order, or a warrant, in terms of what we're able to take.

Again, it's evidence. It's not the privacy part. Where there is private information, that is set aside, protected and destroyed once the investigation has concluded.

Ms. Lori Idlout: Thank you.

This is for each of you as well, and maybe in the same order.

When it comes to doing privacy impact assessments, focusing, of course, on the processes, understanding what your responses are, have you seen the need for updates in legislation or regulation in order for the work you're doing in privacy impact assessments to be completed in a more efficient way?

Mr. Donald Walker: I'm not certain that we would see it as our place to comment on the Privacy Act itself. As an enforcement organization, we are responsible for taking the laws and regulations as they are written and making sure that we are acting accordingly.

I think what we have found is similar to what the Privacy Commissioner said during his testimony, that it is a resource-intensive activity to undertake a privacy impact assessment. We're prepared to put the appropriate resources against it. From our perspective, it's a matter of making sure we have the right expertise in place to help us identify places where putting a better written assessment around our procedures that are in place or refining our procedures is valuable for us to ensure that we have the confidence of the public in how we're using information.

Mr. Brent Napier: I believe the mechanisms in place within the government, within the act, within the law and within the policy are appropriate. I think departments can use those. A PIA is an identified tool to assess risk and to support and inform process change as necessary. We heard from other members about the proportionality of it. It allows us to assess that as well.

In the case of Fisheries and Oceans, it's about managing a public resource, allowing access to a certain group to be able to use the sustainable resource and ensuring that it's being done appropriately on behalf of Canadians. These tools are put into place to ensure and verify compliance for that very important reason.

Ms. Lori Idlout: I think I still have some time.

To each of you, what measures have you taken to ensure the privacy of the data and to prevent misuse of that software?

The Chair: Could you give very quick responses, please?

Ms. Hannah Rogers: We keep a wall between what our forensic investigators find within the use of these tools and the actual investigation that is being completed, so they do not share anything that is not relevant or should not be included in the warrant with the actual investigators. That is one rule.

Also, we destroy any private information that we might discover when we are going through any equipment that we find. We follow international standards for that. As well, our officers are highly trained on exactly how to deal with private information when they do come across it.

● (1140)

The Chair: Thank you.

I'm going to give Mr. Napier a quick 10 seconds.

Mr. Brent Napier: Regarding people processing tools, we have safe storage. We have individuals who are trained. We restrict access and have a process and policy, and we make sure that information is safeguarded.

It's treated as evidence. It's coupled to the same process, which is a very strict process, to allow us to take it to court in a successful way.

The Chair: Thank you for that, Mr. Napier.

That finishes our first six-minute round. We're going to start with our second round of five, five, two and a half, and two and a half.

Mr. Kurek, you have five minutes. Go ahead, please.

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

It's been very enlightening to hear the comments from our witnesses here today, and even that ECCC would consider themselves just another law enforcement agency. Certainly I think that conflicts with what most Canadians would expect of the Department of the Environment.

First to ECCC, have tools capable of extracting personal data ever been used in a situation where there was not judicial authorization? Is there ever an instance where they have been used where there was not judicial authorization?

Mr. Donald Walker: Not at Environment and Climate Change Canada.

Mr. Damien Kurek: Okay, so there has never been an instance.

Mr. Donald Walker: These tools have never been used at Environment and Climate Change Canada without a court order.

Mr. Damien Kurek: Okay.

To the folks at DFO...?

Mr. Brent Napier: It is the same at DFO.

Mr. Damien Kurek: Okay, so you're both saying there has never been an instance where there was not judicial authorization to use these tools.

Mr. Brent Napier: I'm sorry.... Maybe I'll have my colleague comment on an outside the enforcement use of the tool, because there might....

Mr. Damien Kurek: Just keep it brief.

Mr. Sam Ryan: Again, for administrative investigations...and we're not talking about doing something without the knowledge of the employees. Within an administrative investigation that comes through the chief security officer, we have the terms of reference and then the actual employee is fully aware and part of that process, so if there is an investigation they may provide their laptop and their phone with their passwords as well.

Again, it is not used to break into the phone if that's the heart of the question, and no, we do not break into someone's phone. It is done with the understanding and the aid of the employees involved.

Mr. Damien Kurek: Just to give a chance to ECCC, in the course of administrative investigations of employees, has there ever been an instance?

Mr. Donald Walker: It is not currently possible for this tool to be used for administrative investigations at Environment and Climate Change Canada. It is not attached to the network, and it is used exclusively within the enforcement branch.

Mr. Damien Kurek: Okay. Thank you for that.

There is concern around the privacy impact assessment. Certainly I hear from constituents often who will look at a job advertisement they see through ECCC, and it looks like the minister is hiring climate police who may target a farmer. Certainly that has led to an incredible erosion of trust in our institutions, and certainly the people I speak with have very little trust in what this government is doing.

As well, when the Privacy Commissioner was here, I asked very specifically about whether or not he would be able to provide advice to departments that were interested in ensuring they were compliant. The Treasury Board rules indicate that PIAs are not an option. There are some questions about whether they're a legal requirement, but the regulations say very clearly....

It baffles me as to why there would not be pre-emptive work done to ensure that Canadians' rights and privacy are protected.

In 20 seconds or so, I'll start with DFO. Why was a PIA not done beforehand?

Mr. Brent Napier: I think you've heard that many of these tools are long-standing, so 2013 was when DFO first started to use them. At that time there was a different environment. There were rigorous measures taken to secure and ensure that privacy was respected.

Mr. Damien Kurek: Thank you for that, but a PIA was not done before this most recent tool was purchased. My unsolicited advice to you and your superiors, which I would encourage you to pass on, is do the PIA, call the Privacy Commissioner and get it done.

I'll give ECCC the same opportunity.

● (1145)

Mr. Donald Walker: Certainly, I think the Treasury Board directive associated with privacy impact assessments appears to have been viewed, at the time, as not applicable to this particular work because it was not intended to collect, store or treat personal information. As a result of a more comprehensive review undertaken in 2022, the decision was undertaken to complete privacy impact assessments across areas of our work.

Mr. Damien Kurek: I'm basically out of time here. Again, I'm going to give unsolicited advice: Do the assessment. Pick up the phone. To your superiors, pick up the phone and call the commissioner, because right now Canadians do not trust what agencies and departments of this government are doing. They do not trust them with their private information, and when possibly misleading information is being provided to reporters, which has been acknowledged here today, there are a whole host of reasons as to why that trust seems not capable of being extended to this government. Please pick up the phone and do the work beforehand.

The Chair: You are out of time, Mr. Kurek. Thank you.

Mr. Housefather, go ahead for five minutes.

Mr. Anthony Housefather (Mount Royal, Lib.): Thank you, Mr. Chair.

This government has been mentioned multiple times. You bought the software in 2013. Is that correct?

Mr. Donald Walker: Yes. We established the computer forensics unit in 2013.

Mr. Anthony Housefather: Who was the prime minister in 2013?

Mr. Donald Walker: It was a different prime minister in 2013.

Mr. Anthony Housefather: It was Stephen Harper. Thank you very much.

When did you buy the software?

Mr. Brent Napier: It was in 2013 as well.

Mr. Anthony Housefather: Who was the prime minister in 2013?

Mr. Brent Napier: It was Stephen Harper.

Mr. Anthony Housefather: At that time, the requirements were the same—to do a PIA—so obviously, if you're going to blame the Treasury Board president, whoever was Treasury Board president at that time is the one who should be accountable. Thank you very much.

Now let's get to the real chase of things. We're doing this study because people are worried that there is some type of.... The original CBC article that Mrs. Kusie read from talked about spyware. Spyware is a surreptitious thing that you're putting on somebody's phone to extract information on an ongoing basis, to use for nefarious purposes. Do you guys use spyware at all, or malware?

Mr. Donald Walker: No, and I can pass it to my colleague for greater detail.

Unlike spyware, the tools that we use are for the extraction of existing data under a specific court order and with the owner's knowledge. It is not clandestine. It is not ongoing. There is no software installed on the device, and it is not conducted remotely. There's no ongoing component, which would be required for it to be spyware.

Mr. Anthony Housefather: At Fisheries and Oceans, is it the same?

Mr. Brent Napier: It's exactly the same answer, yes.

Mr. Anthony Housefather: The correct word for this would be an extraction tool. Is that right? It's something that you have in a secure location, and you need the device to extract the information, so somebody has voluntarily surrendered their device in each and every case or had a court order to order the production of that device. You then take the information off the device, but then you don't put some program on the phone so that, when it goes back to that person, on an ongoing basis you can take away their information again. Is that correct?

Mr. Donald Walker: That is correct, except that in Environment and Climate Change Canada's case it is not a voluntary submission.

Mr. Anthony Housefather: You do not also use it for employee discipline or violations of codes of conducts by employees, where at Fisheries and Oceans that is a possibility. For you, it's a court order. For you, either it's a court order, or it's voluntary surrender based on an agreement with the employee concerned.

I would imagine that at Fisheries and Oceans... Let's get into that because the other departments so far have generally said, or there are some that have said, that they use it for internal.... Once at the RCMP...but mostly they don't. In your case at Fisheries and Oceans, when somebody signs up as an employee, is it clear in the policies that the device could be used in this way?

Mr. Sam Ryan: Every time you log into the network we have an acceptable use policy. Every time you reboot your computer you access via a virtual private network—a VPN—the acceptable use policy. You accept it. It details what you can and cannot do. Again, these are not Department of Fisheries and Oceans policies. These are Government of Canada policies, so we are applying all of those policies.

Mr. Anthony Housefather: I just want to get back to some terms that got used in the first round, which I think were maybe misinterpreted by people. I just want to come back to them.

You, sir, had talked a little bit about surveillance and surveilling Canadians when Ms. Khalid asked that question. It seemed frightening at the time because it made it sound like we were using technology, because this is all about using technology to surveil Canadians. That's not at all what you meant. Is that right?

● (1150)

Mr. Brent Napier: Fishery officers do monitoring, control and surveillance of the fishery, so there are Canadians active in the fishery—

Mr. Anthony Housefather: But they're not using this technology to do it.

Mr. Brent Napier: That's exactly right; I was not clear.

Mr. Anthony Housefather: We have to be clear. What you're talking about is a hundred-year-old practice where Fisheries and Oceans is out there on the ocean looking to make sure that people are not fishing in places they're not allowed to fish or doing things that are against the law. It's the same visual surveillance that has been going on before any of us were born. Is that correct?

Mr. Brent Napier: That is correct, sir. I would suggest that there are some modern technologies such as an aircraft, but yes, it's definitely not these tools.

Mr. Anthony Housefather: Aircraft existed before any of us were born.

Hon. Robert Oliphant (Don Valley West, Lib.): I'm old.

Mr. Anthony Housefather: If you were born before the Wright brothers, Rob, I'd be surprised.

Can you just clarify that nobody is surveilling Canadians, sir, at Environment Canada?

Mr. Donald Walker: Again, we would not be using these tools to conduct surveillance activities. We may conduct surveillance activities like in the example I used, which was disrespect for the migratory birds regulations in terms of hunting. Generally speaking, compliant hunters would report that to us, and we may watch the site to determine who is engaged in activities.

Mr. Anthony Housefather: That's visual watching.

Mr. Donald Walker: That's correct.

Mr. Anthony Housefather: Thank you.

Thank you, Mr. Chair.

The Chair: Thank you, Mr. Housefather.

[*Translation*]

It's Mr. Villemure's turn now, and he will be followed by Ms. Idlout, and then some Conservatives and Liberals. Each round will be for two and a half minutes. That will be the end of testimony for today.

Mr. Villemure, you have the floor.

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

I find it interesting that my colleague should say that we do not monitor Canadians. Indeed, it's clear to me that none of my colleagues are monitoring the population. There is nevertheless a form of surveillance in the contexts that were mentioned.

Mr. Napier, when people from the RCMP testify before the committee, they often tell us that they use data from cellular telephones. It today's equivalent to what used to be done with a hidden microphone and a lamp. The difference is that much more information can be obtained from a telephone than a microphone hidden in a lamp. The technology is taking us in a completely different direction.

You said earlier that you had started conducting privacy impact assessments in December.

[*English*]

Mr. Brent Napier: That's correct.

[*Translation*]

Mr. René Villemure: I really like your answers so far, but I'm wondering whether you're tempted to balance the need for an investigation against privacy. Before you answer, I'm going to bet on the investigation.

[*English*]

Mr. Brent Napier: I would argue that it is not, in fact, the case. I think we do everything to protect privacy, and that's why we get a judicial authority to go. We make a case, and we present the case to a judge who examines the evidence that we have before us and then provides us strict parameters in terms of what we can and cannot collect, all for the purpose of presenting, beyond a reasonable doubt, a case to a judge.

[*Translation*]

Mr. René Villemure: Do you believe that the Privacy Commissioner could disagree with a judge's authorization?

[*English*]

Mr. Brent Napier: I wouldn't want to speak for either of the two. Certainly they could have their own opinions, but I think the legal system is well constructed in the sense of protecting Canadians and that information. In fact, the evidentiary chain of custody, etc., is probably the most strict; therefore, any information that might accompany evidence would be treated in a similar manner.

[*Translation*]

Mr. René Villemure: Do you think that the commissioner's requirements, at some point in the course of an investigation, might be more of a nuisance than anything else once you've obtained a court order?

[*English*]

Mr. Brent Napier: Not at all. In fact, we're happy to hear any advice or recommendation from the commissioner and evaluate our own processes to ensure that we're respecting privacy within our processes.

[*Translation*]

Mr. René Villemure: Thank you very much.

The Chair: Thank you.

[*English*]

Ms. Idlout, you have two and a half minutes. Go ahead, please.

Ms. Lori Idlout: *Qujannamiik*.

I have three questions, so rather than asking them to respond quickly, what I would like to request is that they provide written responses to the questions that I'll be asking, if that's okay with you.

The Chair: Yes, that's fine. If you want to pose the questions, we'll have the clerk follow up with you on what the questions are.

Go ahead.

Ms. Lori Idlout: Thank you.

Section 5.1 of the directive on privacy impact assessment provides that a privacy impact assessment must be done for “new or substantially modified programs and activities involving the creation, collection and handling of personal information”.

My three questions are these: Could you explain the process that allows you to make a clear distinction between a new and existing program or activity? Second, could you explain the process that allows you to determine if modifications made to a program involving the creation, collection and handling of personal information are important enough to require a PIA? Finally, if you have doubts regarding the application of the directive on privacy impact assessment, do you consult the Treasury Board to clarify the application of its directive?

Qujannamiik.

● (1155)

The Chair: Thank you, Ms. Idlout. I just turned to the analyst and said what an efficient way that was to use the two and a half minutes. It really was.

I would ask that those responses be submitted to the committee by five o'clock on Wednesday. That's in six days, if that's okay. Thank you.

We'll keep it really tight on the timelines and go with two and a half minutes and two and a half minutes, because we have the next panel.

Mr. Brock, you have two and a half minutes. Go ahead, please.

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

In typical Liberal fashion, they often love to blame previous administrations, notwithstanding the fact that they've been in government for almost nine years. They can never accept their own failings.

This question is for both entities. Thinking back on the evidence I have heard, both your organizations have had this device and software for almost 11 years now. I would think that, within that time frame, you've probably conducted hundreds, if not thousands, of investigations using the device and software.

Is that fair to say, Mr. Walker?

Mr. Donald Walker: While it is true that we have conducted a large number of investigations, only 45 of these in the past 11 years have used the computer forensics tools we're discussing.

Mr. Larry Brock: Thank you.

Mr. Napier, it's good to see you again.

Mr. Brent Napier: It's always a pleasure, sir.

Mr. Larry Brock: What's your response?

Mr. Brent Napier: I couldn't give you an exact number, but I know that over the last number of years it's been about 50 cases per year.

Mr. Larry Brock: Okay.

You also understand that the directive by the Treasury Board was not optional. A directive means it must be done.

You've confirmed to Madame Bureau of the CBC that notwithstanding her investigation...which was a great investigation. We wouldn't even know about this—Canadians wouldn't know about this and parliamentarians wouldn't know about this—but for the good actions by Professor Light and the CBC to uncover this scandal. You've confirmed with her that you've never used a PIA on any of those investigations you've identified. Is that correct?

Mr. Brent Napier: That's for the tools. There's a process-level PIA and then there are the tools themselves. There's a differentiation.

Mr. Larry Brock: You confirm that you've never used a PIA.

Mr. Brent Napier: We have PIAs for the larger program, but we haven't adapted it—

Mr. Larry Brock: Right.

Mr. Walker—no PIAs as well. Is that correct?

Mr. Donald Walker: It is correct that we have not had a privacy impact assessment for the use of this tool.

Mr. Larry Brock: Okay.

You know that Cellebrite, one of the manufacturers of this software, makes it abundantly clear that it must be used with the consent of the person you are surveilling. You may be opposed to the concept of spyware, but that's exactly what you're doing. You are spying on Canadians and/or your employees.

I'd like to hear from you, Mr. Napier and Mr. Walker, very quickly. What is your definition of consent?

The Chair: It has to be really quick, please, both of you.

Mr. Brent Napier: It's court-ordered consent, or it could be a witness who provides some form of electronic device. Even in those cases, we still seek a court order to access them.

Mr. Larry Brock: Mr. Walker...?

Mr. Donald Walker: Based on our procurement from the manufacturer, it requires consent or a court order. We would only operate under a court order. Once we have moved from an inspection into an investigation, we would not necessarily ask the regulatee to provide information that would be self-incriminating voluntarily.

The Chair: That's it. Thank you. I appreciate that.

Ms. Khalid, I'll add a little bit extra to your two and a half minutes. Go ahead, please.

Ms. Iqra Khalid: I appreciate that, Mr. Chair. Thank you.

I have two questions for each of you. First, under what circumstances did you acquire this forensic technology 10 years ago under Stephen Harper's government?

Mr. Donald Walker: I will pass it to my colleague shortly.

At the time we procured it in 2013, the circumstances were that many of our regulatees had moved from paper storage of documents into electronic storage of documents. That meant that, in order to retrieve the information we might get out of a filing cabinet in previous times, we actually needed to gain access to electronic devices to develop the evidence necessary to pursue the investigation.

● (1200)

Ms. Iqra Khalid: Thank you.

Go ahead, Mr. Napier.

Mr. Brent Napier: It's very similar. When committing an offence with technology, that technology then becomes subject to these tools. It becomes evidence. It collects evidence. It's not unlike a filing cabinet. This is the new filing cabinet. In order to access that filing cabinet, which could have a lock on it, even in old times, we need these tools. That's how we use them.

Ms. Iqra Khalid: Mr. Napier, when do you expect to have this PIA completed?

Mr. Brent Napier: Like our colleagues from ECCC, it will be this coming fiscal year. We've already made some headway in that direction.

Ms. Iqra Khalid: Mr. Walker...?

Mr. Donald Walker: We expect to have the privacy impact assessment associated with this technology completed by the end of the coming fiscal year.

Ms. Iqra Khalid: Thank you very much.

Those are my questions, Chair.

The Chair: Thank you, Ms. Khalid.

That concludes our first panel.

I want to thank Mr. Walker, Ms. Rogers, Mr. Napier and Mr. Ryan for appearing before the committee on this important subject.

We are going to suspend for a couple of minutes and go to the next panel. The meeting is suspended.

● (1200)

_____(Pause)_____

● (1205)

The Chair: I call the meeting back to order for our second hour today.

I'd like to welcome our witnesses. From the Canada Revenue Agency, we have Eric Ferron, director general, criminal investigations directorate, compliance programs branch; and Anne Marie Laurin, acting director general and deputy chief privacy officer, access to information and privacy directorate, public affairs branch. From the Canadian Radio-television and Telecommunications Commission, we have Steven Harroun, chief compliance and enforcement officer; and Anthony McIntyre, general counsel and deputy executive director, legal services.

We're going to start with the Canadian Radio-television and Telecommunications Commission.

You will have up to five minutes to address the committee. Go ahead, please.

● (1210)

Mr. Steven Harroun (Chief Compliance and Enforcement Officer, Canadian Radio-television and Telecommunications Commission): Good afternoon and thank you for inviting us to appear before your committee.

Before I begin my remarks, I would like to acknowledge that we are gathered on the traditional, unceded territory of the Algonquin Anishinabe people.

My name is Steven Harroun. I am the chief compliance and enforcement officer at the CRTC.

[*Translation*]

I am joined today by the CRTC's general counsel, Anthony McIntyre.

The CRTC is an independent, quasi-judicial tribunal that operates at arm’s length from the government. We hold public hearings on telecommunications and broadcasting matters, and we make decisions based on the public record.

[*English*]

In addition, the CRTC plays a part in a larger federal government effort to protect Canadians from spam, malware, phishing and other electronic threats. The CRTC is one of three agencies, along with the Competition Bureau and the Office of the Privacy Commissioner, that work to promote and enforce compliance with Canada's anti-spam legislation, or CASL, as we call it.

The CRTC has a small team of less than 20 people that carries out this important mandate. CASL authorizes our investigators to request warrants from the courts to examine computers and other electronic devices when necessary. As part of those authorized activities, CRTC staff can use digital forensic tools during investigations. How we use these tools is very limited in scope and is done in keeping with the law. In the very limited circumstances in which we have used these tools, we have obtained judicial authorization through the courts in the form of a warrant.

Since 2022, the CRTC has only used these tools in two CASL investigations. In these cases, a warrant was obtained and the CRTC was successful in uncovering evidence related to potential CASL violations.

[*Translation*]

We take the use of digital forensics tools very seriously. We follow strict legislative and judicial parameters when using these tools.

[*English*]

Thank you for allowing us time to explain our limited use of these tools to help protect Canadians from harmful electronic threats.

We look forward to your questions.

The Chair: Thank you, Mr. Harroun. You're well under time, which the committee appreciates.

We're going to the Canada Revenue Agency now.

You have up to five minutes to address the committee. Go ahead, sir.

Mr. Eric Ferron (Director General, Criminal Investigations Directorate, Compliance Programs Branch, Canada Revenue Agency): Thank you, Chair.

Thank you to the Standing Committee on Access to Information, Privacy and Ethics for having us here today. My name is Eric Ferron, and I am the director general of criminal investigations at the Canada Revenue Agency, the CRA. I am accompanied by my colleague, Anne Marie Laurin, acting director general of the access to information and privacy directorate, and deputy chief privacy officer.

Within the scope of my responsibilities, the criminal investigations program investigates significant cases of tax evasion, tax fraud and other serious violations of tax laws and, where appropriate, refers cases to the Public Prosecution Service of Canada, the PPSC, for possible criminal prosecution.

Ms. Laurin's responsibilities include providing strategic direction, expert advice and leadership on all access to information and privacy matters in support of the CRA's programs, services and priorities.

I would like to start by stating that the CRA does not use spyware tools to monitor its employees or Canadians. The criminal investigations program does use the technological tools that are the topic of today's discussion.

CRA criminal investigators and computer forensics analysts are public officers as defined by section 2 of the Criminal Code. As public officers, CRA investigators can obtain evidence during the conduct of a criminal investigation by way of search warrants, preservation orders and production orders pursuant to section 487 of the Criminal Code. This is in addition to the search powers provided by the acts administered by the CRA.

Warrants issued by the court grant authority to CRA investigators to search and seize personal information or data that could otherwise be protected by section 8 of the Canadian Charter of Rights and Freedoms. In granting a search warrant, the issuing justice or judge must balance the rights of the CRA to gather evidence as part of a criminal investigation with the rights of individuals. Under section 487 of the Criminal Code, search warrants are sought when there are reasonable grounds to believe that an offence has been or is suspected of having been committed.

The evolution of technology has expanded the use of search warrants beyond traditional physical locations. Subsections 487(2.1) and 487(2.2) of the Criminal Code speak to search warrants of computers and electronic data, allowing the CRA investigators to search the electronic devices they have seized for data. It is during the execution of these judicial authorizations that the CRA may use technological tools to extract data from electronic devices.

A privacy impact assessment for the criminal investigations program has been in place since 2016, and the CRA was in the process of finalizing updates to it in late 2023. The update to the assessment has now been finalized, and in line with best practices the program intends to continue reviewing its PIA on a regular basis to ensure it is up to date and reflects current operations.

Mr. Chair, this concludes my opening remarks. Ms. Laurin and I would be pleased to answer any questions that committee members may have.

● (1215)

[*Translation*]

The Chair: Thank you, Mr. Ferron.

We are now starting the first round of questions.

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

[*English*]

Mr. Michael Barrett (Leeds—Grenville—Thousand Islands and Rideau Lakes, CPC): Chair, I'm going to take this opportunity to give a notice of motion that will be moved at a later meeting. It reads:

> Given that the former President of Sustainable Development Technology Canada testified before committee last week, claiming that the Minister of Industry knew about conflicts of interest at the taxpayer-backed fund since 2019, contradicting the minister's claim that he found out about abuse at the fund just this year, and that senior government officials misled committee about their attendance at SDTC board meetings where conflicts of interest occurred by board directors and the CEO by directing taxpayer money to companies that they have an interest in, and that a senior Department of Industry official who oversaw an investigation into the fund compromised the investigation through interference and unethical behaviour, the committee dedicate five meetings related to developments at Sustainable Development Technology Canada.

I can send that text to the clerk, Chair, but this is an incredibly important issue. When I have the opportunity to move it at our next meeting, with notice having been given, I would encourage all members to consider over the next couple of days their support for it, because this is an incredibly important issue.

The Chair: Thank you, Mr. Barrett, for that notice of motion. Once it is sent to the clerk, it will be put into the digital binder for committee members to have a look at.

Mr. Barrett, you have four minutes and 40 seconds. Go ahead, please.

Mr. Michael Barrett: I'll give my time to Mrs. Kusie, please.

[*Translation*]

The Chair: In that case, it's over to you Ms. Kusie.

[*English*]

Mrs. Stephanie Kusie: Thank you very much, Mr. Barrett, and thank you very much, Chair.

I'm going to again quote the Privacy Commissioner, who said that it's going to be “even more important to reassure Canadians” and that “we need to have that reflex of privacy by design and privacy at the front end.”

I must say, I was not quelled by the first group of departments that were here this morning. What I heard was, “We did not have the PIAs. Don't worry. We didn't use them on employees, but we used them in far more extensive and invasive other places.” I'm very concerned by that.

I will say that the committee agreed to communicate with all 137 federal institutions. It's unfortunate that, for these four organizations that are here today as models and as sort of a check on the other departments, this is the pressure that is on them this morning.

The last comment I'll make before I get to the questioning is that I find it ironic that the Privacy Commissioner actually learned of the invasion, if I can use that term, by the federal departments and agencies, from the government agency of Radio-Canada, which first posted this story. I think this is another very ironic piece of information, given this meeting this morning.

I'll start with you, Mr. Harroun, with the same question I used with your previous colleague.

Did your department procure surveillance gear that can be used to access employees' information and potentially the information of Canadians at large?

● (1220)

Mr. Steven Harroun: No, we do not procure surveillance gear. We have digital forensic tools, which we use to enforce CASL.

Mrs. Stephanie Kusie: Do these digital forensic tools require the PIA?

Mr. Steven Harroun: They do.

Mrs. Stephanie Kusie: Was the PIA obtained for these tools prior to their use?

Mr. Steven Harroun: When CASL came into force in 2014, the CRTC conducted three PIAs, as it was a brand new program. One of those PIAs specifically references section 19, which is search warrants and the use of digital forensic tools. We've had a PIA since 2014.

Mrs. Stephanie Kusie: You have valid PIAs for all of these tools that you are currently using.

Mr. Steven Harroun: That's correct.

Mrs. Stephanie Kusie: Okay.

I'll ask the same question of Mr. Ferron.

Did your department procure surveillance gear that can be used to access employees' information and potentially the information of Canadians at large?

Mr. Eric Ferron: Criminal investigations has tools that we're discussing here today. They're not surveillance tools. They are digital forensics tools that we use as part of our criminal investigations.

We've had a PIA for the criminal investigations program as a whole since 2016. The tools that we have were purchased right before that.

Mrs. Stephanie Kusie: Have you received any direction from the Treasury Board when it was announced that many departments were not in compliance with the required PIAs, Mr. Ferron?

Mr. Eric Ferron: The discussions with the Privacy Commissioner happened with my colleague here, so I'll let her address that question.

Ms. Anne Marie Laurin (Acting Director General and Deputy Chief Privacy Officer, Access to Information and Privacy Directorate, Public Affairs Branch, Canada Revenue Agency): Thank you for the question.

Both the OPC and Treasury Board sent follow-up questions regarding that. We indicated that we use the forensic tools for the purposes of criminal investigations. We did have a PIA in place. In fact, the Privacy Commissioner acknowledged receipt of that PIA and had no recommendations on it at the time.

Mrs. Stephanie Kusie: I will also ask Mr. Harroun if he received any direction from the Treasury Board when it was announced that other federal departments didn't have the required PIAs.

Mr. Steven Harroun: We did not receive a direction from the Treasury Board. We advised Treasury Board that we had a PIA, as per my previous answer.

Mrs. Stephanie Kusie: Would both departments be aware that, if the President of the Treasury Board was made aware of a systematic compliance issue, they are able to make direct recommendations to the head of the government institutions involved?

Were there are no PIAs?

The Chair: Answer very quickly, both of you—either a yes or no, if you can do that.

Ms. Anne Marie Laurin: PIAs are submitted to both Treasury Board and the OPC, so they have an opportunity to provide feedback to us on those things.

Mrs. Stephanie Kusie: Thank you, Chair.

The Chair: Thank you.

We'll go to Mr. Housefather for six minutes.

Go ahead, please.

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

While I always appreciate my colleague Mrs. Kusie, I think I was at a different panel than her for the first panel, because I didn't hear any of the things that I think she heard.

I mean, I think when we came here today some people were hoping to hear that these tools were bought since the Liberals took power in 2015—

Mrs. Stephanie Kusie: I have a point of order, Mr. Chair.

Perhaps, if the clerk can check the attendance from the first hour, the clerk will recognize that I was here. Maybe we can take a moment to verify the attendance for the first hour.

The Chair: I don't need her to do that. I know you were here.

Mrs. Stephanie Kusie: Okay. Thank you very much, Mr. Chair.

The Chair: Go ahead, Mr. Housefather.

Mr. Anthony Housefather: I didn't say you weren't here. I said I didn't think we were at the same meeting. I didn't say you weren't here.

Mrs. Stephanie Kusie: I have a point of order, Mr. Chair.

Mr. Anthony Housefather: You described the first panel differently than I perceived it.

The Chair: Mr. Housefather, I have another point of order from Ms. Kusie.

Go ahead.

Mrs. Stephanie Kusie: I believe the member across from me was implying that I was absent from the room for the first hour, when in fact—

Mr. Anthony Housefather: No, I wasn't.

Mrs. Stephanie Kusie: That was the implication. That was the implication.

Thank you, Mr. Chair.

The Chair: That's a matter of debate.

I'll go to you, Mr. Housefather. I stopped your time. Go ahead.

Mr. Anthony Housefather: I'm not even going to get into that one.

Thank you, Mr. Chair.

I think there was an attempt to somehow say that these tools were bought when the Liberals were in power, no PIA was obtained and there was negligence on the part of the Treasury Board.

To the CRTC, just to be clear, when did you buy the tool?

Mr. Steven Harroun: We bought it in 2014.

Mr. Anthony Housefather: It was in 2014, before the Liberals took power.

[*Translation*]

What about the Canada Revenue Agency?

[*English*]

Mr. Eric Ferron: It was 2012.

Mr. Anthony Housefather: Okay.

Then, as to a PIA, there was an attempt to say, well, you guys didn't comply. There was no PIA.

To the CRTC, you do have a PIA for this program.

● (1225)

Mr. Steven Harroun: Since 2014.

[*Translation*]

Mr. Anthony Housefather: Hasn't the Canada Revenue Agency also had a PIA since 2016?

Mr. Eric Ferron: That's correct.

[*English*]

Mr. Anthony Housefather: It sounds like you guys are in compliance, which is good to hear.

I guess the other thing that may have been of more general concern was how these tools were being used. Were these tools being used to somehow surreptitiously spy on Canadians? From what I understand, neither CRTC nor Revenue Canada is using spyware or malware or inserting tools on devices to do anything nefarious.

Would that be correct, CRTC?

Mr. Steven Harroun: That would be correct.

[*Translation*]

Mr. Anthony Housefather: Is that also the case for the Canada Revenue Agency?

[*English*]

Mr. Eric Ferron: That is correct, yes.

Mr. Anthony Housefather: Perfect.

I understand that the way in which you use these tools is simply to extract data from the device that you have in your possession.

To the CRTC, is that true?

Mr. Steven Harroun: That is correct.

[*Translation*]

Mr. Anthony Housefather: Is that also the case for the Canada Revenue Agency?

[*English*]

Mr. Eric Ferron: Yes, and it's only once we have a judicial order.

Mr. Anthony Housefather: I was going to get to that in my next question.

To the CRTC, would you also confirm that you would need, and you've always gotten, a warrant before the taking of a device?

Mr. Steven Harroun: Every time we obtain a device and/or use this tool, we have a search warrant that specifies the use of these tools.

Mr. Anthony Housefather: The other thing that I would imagine we were also seeking to do was to confirm that you weren't outrageously using these devices by having outrageous numbers of warrants for Canadians to have to produce things.

To the CRTC, I think you said that you've used this only twice since 2013.

Mr. Steven Harroun: Since 2022 we've used it twice. Overall, we've used it a handful of times in 10 years.

Mr. Anthony Housefather: You were not using this on an absolutely regular and ongoing basis.

Mr. Steven Harroun: It has a very limited scope in a very limited type of investigation.

Mr. Anthony Housefather: You're not using it with respect to internal matters at the CRTC, where employees are being disciplined for violating internal policies.

Mr. Steven Harroun: It is only used for CASL investigations and for a very specific type of CASL investigation. There is limited use of that tool. Even within my own team, there are only four or five technical experts who even know how to use it.

[*Translation*]

Mr. Anthony Housefather: Can I ask the Canada Revenue Agency the same question?

Mr. Eric Ferron: At the Canada Revenue Agency, we only use that tool for criminal matters when we have judicial authorization. Such authorization also allows us, once we have seized a device, to use the tool to gain access to its contents and withdraw information. That's the only use we make of the tool.

Mr. Anthony Housefather: Okay, great.

[*English*]

I'll now go through process questions, because I think that was another thing. I'll keep alternating between you.

Does CRTC generally try to comply with Treasury Board directives? When regulations come through Treasury Board and when there are directives from Treasury Board, is there an effort to comply, usually?

Mr. Steven Harroun: I would suggest “yes”.

Mr. Anthony Housefather: How do you ensure that you are compliant? What method do you use to review it? I imagine that you have people at CRTC who are responsible for ensuring that these directives are being complied with. How does that work?

Mr. Steven Harroun: Absolutely. We have a strong corporate team at the CRTC that looks at all the directives across government, be it the Treasury Board, the Privacy Commissioner or others. If it impacts my program and the work that we do, then I am directly involved in ensuring that we meet all those requirements.

[*Translation*]

Mr. Anthony Housefather: I'm going to ask the Canada Revenue Agency's representatives the same question. How do you ensure compliance with directives?

[*English*]

Ms. Anne Marie Laurin: We have a privacy management framework in the agency. We have a chief privacy officer as part of that privacy management framework. The pillar is privacy by design.

We monitor the completion of things like privacy assessments. In fact, we have key performance indicators that measure that. Quarterly updates are provided to senior management on the completion of privacy assessments.

Mr. Anthony Housefather: Let's say, not only isolated to this issue but on other issues where you deal with the Treasury Board, there's an ongoing dialogue, as I understand it, between Revenue Canada and the Treasury Board. Is that correct?

Ms. Anne Marie Laurin: Yes, and it's also with the Office of the Privacy Commissioner.

Our privacy management framework takes all dimensions of privacy into account and monitors all portions of that from a policy perspective as well as a practice perspective.

Mr. Anthony Housefather: The vast majority of these interactions would occur at the departmental level. Is that right? They wouldn't be with politicians. It wouldn't be Minister Anand entering your premises to start directing you as to how to apply Treasury Board rules. You deal with bureaucrats at the department.

Ms. Anne Marie Laurin: Yes. Privacy is an obligation of all parts of the agency. Senior management is regularly engaged in those obligations and understands those roles and responsibilities.

Mr. Anthony Housefather: Thank you so much.

I'll ask the CRTC the same thing.

Mr. Steven Harroun: It's the same thing. The CRTC is in compliance with all federal government requirements.

Even more to your point about a minister, we are a quasi-judicial independent tribunal. We're even one step further removed.

● (1230)

Mr. Anthony Housefather: Thank you so much.

I think my time has probably lapsed.

Thank you, Mr. Chair.

The Chair: Yes, it has.

Thank you, Mr. Housefather.

[*Translation*]

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

Mr. René Villemure: Thank you Mr. Chair.

Thanks to everyone for being here.

As you know, this parliamentary committee's work often involves reassuring the population about matters of concern to them, as is the case here.

I'm going to begin with the Canada Revenue Agency's representatives.

People are a bit scared of the Canada Revenue Agency. They don't talk about it much. They prefer to have it behind them rather than in front of them. That's why trust is so important. Trust is how we feel about someone without any need for evidence. It's spontaneous.

The story published by the CBC mentioned that the Canada Revenue Agency had not done a PIA. But your evidence this morning says otherwise. Could you please explain the difference between the two versions.

Mr. Eric Ferron: I can try.

We have indeed had the PIA process in place since 2016. The assessment is for the program as a whole, and not the tools. When we were asked about it, we may not have been as accurate as we might have been with our answer. That may have caused some confusion.

So we have, since 2016, had a PIA in place for the program under which the tools in question are used.

Mr. René Villemure: Do you believe there should be a PIA for the tool in question?

Mr. Eric Ferron: My understanding is that the PIA is for the program. That's why we did what we did. In our assessment, we say that our experts use some tools when electronic devices are seized in order to extract information.

So there really is a PIA and it's been there since 2016.

Mr. René Villemure: It might be useful to tell communications people that they should be very specific. In fact, several witnesses told us that what had been reported did not altogether reflect what they had said, or that they were no longer confident about what they had answered. That's when mistrust begins, when the intent is anything but. And that's not desirable, particularly given that things move quickly when the Canada Revenue Agency is involved.

So my understanding is that the PIA that has been in place since 2016 is for the overall program, not the tool, and that the latter is used under the circumstances that you mentioned.

Mr. Eric Ferron: That's right.

Mr. René Villemure: Okay. Thank you.

Mr. Harroun, I'll ask you the same question.

People are not knowledgeable about the CRTC. They think that all it does is regulate the airwaves, but it does much more than that.

As it turns out, your organization, in response to a journalist's question, said that it had not done a PIA, and you are now saying that this type of assessment has been in place since 2014.

How can the two versions be reconciled?

Mr. Steven Harroun: Thank you very much for the question.

I think we're in the same position as our colleagues.

[*English*]

A big question the reporter asked, I believe, was very specific. It was, “Do you have a PIA for this specific tool?” The response was “no.”

As I indicated, we do have a PIA for the program, which is typically how PIAs work. It's for the entire program where those digital forensics tools are identified. It's not by name. For example, if it became a different name, if it became “Cellebrex” or “Cellebrite 2.0”, then that PIA would no longer be valid. It's for the tools overall.

[*Translation*]

Mr. René Villemure: Would you say that a PIA should be done for the use of a specific tool, or rather that the program covers everything?

[*English*]

Mr. Steven Harroun: I would suggest that the program PIA covers it all, because it is very specific about the use of digital forensic tools and evidence gathering, etc.

[*Translation*]

Mr. René Villemure: Do you believe there are less invasive ways of obtaining the same results?

[*English*]

Mr. Steven Harroun: It would be extremely challenging. For example, we use the digital forensic tools to gather information. For example, we all carry computers in our pockets. At the end of the day, these are now minicomputers. It's not like a laptop computer, where you can remove the hard drive, analyze that hard drive and put it back in. The only way into this phone and to know what's in this phone is to, literally, through this port—which is how Cellebrite works—connect to the phone. It makes a digital copy, a forensic evidentiary valid copy of that phone, and then Cellebrite allows us to analyze it and to preserve it for investigation purposes, for Federal Court purposes, etc.

[*Translation*]

Mr. René Villemure: Thank you very much for your answer.

We are here to legislate. In that capacity, what might we do to allay people's concerns about the use of these sorts of tools, which will certainly increase given the speed with which technology is developing? Concerns like this don't do anyone any good.

What more can you do to reduce their anxiety?

● (1235)

[*English*]

Mr. Steven Harroun: As the regulator, we implement any legislation put forth by parliamentarians. If there were suggestions, be it through the Privacy Commissioner or others, that there should be changes to specific aspects, the CRTC would undertake to meet all those obligations.

[*Translation*]

Mr. René Villemure: Could you provide us with a few suggestions in writing?

[*English*]

Mr. Steven Harroun: Absolutely, I'll undertake that.

[*Translation*]

Mr. René Villemure: Thank you very much.

I have the same question for Mr. Ferron, and the same request for suggestions.

Mr. Eric Ferron: I don't have any suggestions right now. We follow the rules as written. As I said at the outset, many of them are in the Criminal Code. We stick to these rules to ensure that when we use the tool…

Mr. René Villemure: I apologize for interrupting, but I don't have much time.

To strengthen people's trust in the Canada Revenue Agency, do you have any suggestions as to what we, the legislators, might be able to do to help you?

Mr. Eric Ferron: I don't have anything specific for you at the moment.

Mr. René Villemure: Okay.

Thank you very much.

The Chair: Thank you, Mr. Villemure.

[*English*]

Ms. Idlout, you have six minutes. Go ahead, please.

Ms. Lori Idlout: *Qujannamiik* and welcome.

I have, very quickly, some questions for the Canada Revenue Agency related to the article that was originally published by Radio-Canada in November 2023. I'm sure you know what I'm talking about. In that article it was mentioned that the CRA was using tools, and it was using these tools to analyze data related to tax offences.

First, can you explain in more detail how the use of such tools by your institution can be justified under a federal law, if any?

Mr. Eric Ferron: The criminal investigations program is responsible for investigating significant cases of tax evasion. That requires us to gather evidence, and our investigators will use the tools that they have at their disposal to gather this evidence. This can include interviews of suspects and of witnesses, but it can also include the use of judicial authorizations. This can be used for production orders or search warrants.

When we do search warrants, we can come across some electronic devices. We'll need to extract the data from these devices, these computers or cellphones, and it's with these tools we're talking about here today that we can do so. It allows us to get access in a very surgical way and not go through the whole phone by ourselves. The tools allow us to find what we're looking for. This will be used as evidence, ultimately, that we would present to the courts.

Ms. Lori Idlout: If the authority for the use of these tools is not coming from law, where is the source coming from for you to use them?

Mr. Eric Ferron: The authority we have is in the Criminal Code. That is what allows us to use the tool, to seize these electronic devices in order to use the tools to extract the data.

Ms. Lori Idlout: I have questions for both of you, both agencies, because when you were responding to one of the Conservative's questions regarding surveillance, both of you responded to say that you don't generally surveil people, but both of you mentioned that you use digital forensic tools.

Can each of you provide more details about what that actually means? *Qujannamiik*.

Mr. Eric Ferron: For the criminal investigations program at the CRA, the difference is that, when we have a judicial authorization that allows us to do a search, and if we come across an electronic device and we seize this device, we would then be able to extract the data from it. We have to have the tool connected to the electronic device—a phone or a computer—so the process is very limited that way. In other words, we can't be surveilling the Canadian population as a whole. These tools are made to be used with the actual phone, the actual computer or the electronic device that we have seized as part of a search.

Mr. Steven Harroun: I'll explain. There are several provisions under CASL, the anti-spam legislation that we have. Some of those provisions relate to the CRTC's ability to investigate the installation of software without consent, which includes viruses, malware, botnets and those types of activities—the more nefarious activities, if you will. When we're involved in an investigation related to those types of activities, we are often required to seek a search warrant to go collect devices to use this digital forensic tool to....

It comes down to the basics of evidence: We identify, analyze and preserve the evidence, and that's how we use this tool, in those very limited circumstances, on those very specific CASL cases.

● (1240)

Ms. Lori Idlout: *Qujannamiik.*

Because I'm not very familiar with this file, I don't know if there are any reporting requirements of incidences when you've had to use digital forensic tools. Is there data that's collected annually to show how many times each of your agencies has had to use them, and do you report that to Parliament?

Mr. Steven Harroun: For the CRTC, we do not have a reporting requirement. Because our scope and our use is so limited, as I said, it's less than a handful of times in 10 years. It is very specific.

Mr. Eric Ferron: We don't have any reporting requirements on the use of the tools. We do report various statistical data when it comes to criminal investigations, but not in terms of specific use of that tool.

The Chair: Thank you, Ms. Idlout.

That concludes our first round of questioning.

We're going to our second round of five, five, two and a half, and two and a half.

We start with Mr. Kurek. Go ahead for five minutes.

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

Thanks to our witnesses.

This is just an observation. It's interesting. You talked about the PIA, but in the context of the report that triggered this committee to go about this study, I would encourage the idea of “transparency by default” to make sure that it is clear. You're talking about a PIA being done, and certainly an early explanation about that process would have been helpful. I'm sure that the reporters who did the investigation would have valued that information as well.

Just as another observation, both of your departments acquired this technology under a previous government and did the PIA, so certainly there seems to be a deep care for a former president of the Treasury Board's commitment to ensuring that privacy was respected.

To the CRA, I'd like to get some numbers, if I could. How often is this technology to extract data from cellphones used on a yearly basis within your investigations? It's to the CRA in general, but specific to investigations.

Mr. Eric Ferron: I'm sorry, but I don't have the specific information you're looking for. We don't have the specific number of times we've used the tool to extract data from computers or cellphones we would have seized. It's something we can look into and provide that information.

Mr. Damien Kurek: If you can provide that to the committee, I think it would be helpful. Are we talking about dozens, hundreds or thousands of times? There's a massive range of what could be possible, so if you could please provide that in writing to the committee—so that we could make it public—that would be appreciated. Can I ask for that information?

Mr. Eric Ferron: Yes, we'll do our best to gather that information.

The Chair: Just so that we're clear, we work on deadlines here, so by next Wednesday, if possible....

Mr. Eric Ferron: We'll do our best. We've had this tool for several years now. I don't know how far back we can go in terms of providing fulsome numbers, but we'll do our best.

The Chair: Thank you.

Go ahead.

Mr. Damien Kurek: Thank you for that, Chair.

In relation to COVID-related programming—so CERB, for example—I know there were 185 employees, it was reported, who had inappropriately collected CERB cheques. I'm wondering; was this tool used in the process of determining the fault of those 185 employees?

Mr. Eric Ferron: The criminal investigations program does not have the mandate to investigate CERB offences. We do have the mandate to investigate other COVID benefits, and—

Mr. Damien Kurek: Who has the mandate to investigate CERB?

Mr. Eric Ferron: I believe it would be the ESDC or law enforcement.

Mr. Damien Kurek: Okay. Continue with your previous....

Mr. Eric Ferron: The criminal investigations program, if we are investigating an offence of one of these pieces of legislation, we could use the tool to gather information if we've seized an electronic device during a search, but we would not use the tool to do an internal investigation of the actions of people within the agency.

● (1245)

Mr. Damien Kurek: Over the course of COVID, was there...? I guess this is something that you could provide to the committee as well, whether there was an increase in the number of investigations that took place.

When it comes to the invocation of the Emergencies Act, were there any instances during the course of the invocation of the act when this technology was used?

Mr. Eric Ferron: No, not for the CRA.

Mr. Damien Kurek: Okay. Thank you very much. Has there been an instance when it has ever been used without judicial authorization?

Mr. Eric Ferron: No. You need judicial authorization to do your search, and that's when you would seize an electronic device. You have to have judicial authorization.

Mr. Damien Kurek: In terms of safeguards to protect Canadians' data, I know there have been a number of...and it makes headlines when the tax authority gets hacked. I'm just curious if you can outline what some of the safeguards are to ensure that Canadians' data is protected. It's incredibly intrusive to have a copy of someone's cellphone. I'm wondering what safeguards are in place to ensure that Canadians' privacy is protected during the course of an investigation.

Mr. Eric Ferron: When we have a judicial authorization, that allows us to do a search and then we seize an electronic device. This would then be stored in a stand-alone computer, in an area that only our computer forensic analysts have access to. It's not connected to the Internet. It's not connected to the network of the CRA. These stand-alone computers are in a secure area that allows for maximum protection.

Mr. Damien Kurek: Just to wrap up—it's not a question; it's just to make sure—the Privacy Commissioner was here, and he said that phone calls are welcome when asking for advice. I appreciate that there were PIAs done. That's certainly helpful, but make sure that you, your employees and superiors.... The Privacy Commissioner wants to work with you to make sure that the information of Canadians is protected. Certainly, transparency by default is an expectation I would hope we all have for every agency of government.

The Chair: Thank you, Mr. Kurek.

Mr. Bains, you have five minutes. Go ahead, please.

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

Thank you to the agencies for joining us today.

My first question is for the CRA. We heard before how you gather evidence, and if the evidence requires, then the steps are taken to get judicial consent to go in and try to extract information by using these tools. I have just a couple of questions.

How many CRA employees have access to these forensic tools?

Mr. Eric Ferron: We have, in criminal investigations, approximately 700 employees. Approximately half of them are part of the investigative groups, but the computer forensic analysts are a very small subgroup of specialized people who can do this type of work. I don't have the exact number, but that's something we can provide to the committee.

Mr. Parm Bains: Please do, but let's say an investigation takes place. Only a specific number of investigators would be looking at that. Not everybody would have access to these files.

Mr. Eric Ferron: It's only the people who are involved in the investigation. It's on a need-to-know basis, so it's not even all the investigators who would have access. It's only the people who are involved in the file, and actually, the investigators get access to only the information that is relevant. The CFAs—our computer forensic analysts—will sift through the electronic devices and take out what is relevant for the investigation, and that's what the investigators will look at.

Mr. Parm Bains: What's the level of security clearance inside the agency for those who are authorized to access these tools? What are some measures you've taken inside the agency?

Mr. Eric Ferron: Our criminal investigations, the investigators and the computer forensic analysts, have secret clearance, and the information that we have is stored in special areas that only our computer forensic analysts have access to on stand-alone computers. The security on these computers has been assessed to be adequate to protect the information, and the risks appear to be low.

Mr. Parm Bains: Now let's say someone who's not assigned to a case tries to access something. You would be alerted in some manner. You have those measures in place.

● (1250)

Mr. Eric Ferron: Yes, but not me personally. Maybe, ultimately, if there were some wrongdoing—

Mr. Parm Bains: No, but the agency would.

Mr. Eric Ferron: The criminal investigations unit has some processes in place to limit who has access. Outside of criminal investigations, nobody has access to our files.

Mr. Parm Bains: Are these tools used strictly to access data? I think you've already mentioned that it's specific to the cases you've investigated. What about cloud-based databases or data that's out of scope that's accidentally accessed?

Mr. Eric Ferron: The tools we're discussing here today actually help us to ensure that we are thorough but at the same time very precise in what we get out of these computers, telephones or any electronic devices. It allows us to be more surgical, to seek out only what is relevant to the investigation.

When we have our judicial orders, there are terms of references in the actual order that explain what we can get access to, so those are other ways of limiting what we would get our hands on.

Mr. Parm Bains: It's a similar question for the CRTC. I think you demonstrated how someone would access the phone by entering though the wire, or the USB or what have you, to extract. Is there an ability to extract information remotely?

Mr. Steven Harroun: No. This tool does not work remotely. We actually have to connect to the device.

Mr. Parm Bains: You would have to get the warrant, get the approval to obtain the device and then go in without any remote access, connect to the device and extract.

Mr. Steven Harroun: Absolutely. Through our search warrant it identifies what we're looking for and how we will obtain that information using these types of digital forensic tools. That search warrant is explained to the individual when we're executing the search warrant, so they are well aware of what's going to happen. They willingly, or at least by court order, offer us up that device. Even more importantly, often they're required to give us the password. If we don't have the password to that device, we cannot use this tool.

The Chair: Thank you, Mr. Bains.

Thank you, Mr. Harroun.

[*Translation*]

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

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

I'd like to move the following motion, which has been sent to the clerk. It's been translated and sent to everyone. It reads as follows:

> That, in accordance with Standing Order 108(3)(h), the Committee undertakes a study of misinformation and disinformation and their impact on the work of parliamentarians, that the Committee devotes the next three available meetings to this study; that the Committee invites experts in the field of misinformation and disinformation; and that the Committee reports its observations and recommendations to the House.

The Chair: Thank you, Mr. Villemure.

I It was emailed to all the committee members.

I would ask the witnesses to please bear with us for a few seconds while we discuss Mr. Villemure's motion.

Would you like to speak to your motion, Mr. Villemure?

Mr. René Villemure: Yes. Thank you.

Several global think tanks, the most recent being the World Economic Forum, have published alarming information. The latest statistics show that people in general, business people and those working for government departments and organizations, are concerned about disinformation and misinformation.

We've known for some time that they exist. However, it's surprising to learn that the current level of concern is higher than ever and is now comparable to people's anxiety over climate change. It's something rather more subtle, and below the waterline, but it nevertheless has an impact on what parliamentarians think and the decisions they make.

We've now reached a point that requires decisions about matters that affect the population, departments and organizations. In fact, since the arrival of generative artificial intelligence, the concept of truth itself is being challenged, because the true and the false are becoming difficult to distinguish. Under these circumstances, I believe that it's imperative for us to undertake a study of this kind and for us to hear from experts in the field, in order to prepare ourselves to deal with these issues and better serve the public interest.

● (1255)

The Chair: Thank you, Mr. Villemure.

I spoke with the clerk and he hadn't received the notice of motion.

[*English*]

That causes us a bit of a problem here. I may have overstepped my boundary by accepting the motion. If members don't want to discuss the motion, then we'll have to take this as a notice of motion to be discussed at perhaps a later date.

Just as Mr. Barrett did before, if we can take this as a verbal notice of motion—I am very sorry for this, and I appreciate your comments—then perhaps we can discuss it at a future meeting.

[*Translation*]

Mr. René Villemure: That's not a problem, Mr. Chair.

The Chair: Thank you, Mr. Villemure. Allow me to apologize once more.

You still have the floor for a minute and a half, if you wish.

Mr. René Villemure: Certainly.

Good day once again to the witnesses.

Very briefly, Mr. Harroun, do you feel it would be appropriate to amend the Privacy Act to reflect these new realities?

I'd also like to hear from Mr. Ferron on this.

[*English*]

Mr. Steven Harroun: If it is deemed that the Privacy Act should be amended for whatever reason, we will comply with those amendments.

[*Translation*]

Mr. Eric Ferron: I agree with my colleague.

Mr. René Villemure: Do you have any suggestions with respect to amending the act?

Mr. Eric Ferron: I don't have any comments on this for the committee today.

[*English*]

Mr. Steven Harroun: I have no suggestions.

[*Translation*]

Mr. René Villemure: Thank you very much.

The Chair: Thank you, Mr. Villemure.

[*English*]

Ms. Idlout, you have the final two and a half minutes. We'll adjourn the meeting after that.

Go ahead, Ms. Idlout.

Ms. Lori Idlout: *Qujannamiik.*

I will also be asking for responses in written form. Having heard your responses to my Bloc colleague previously, I invite you to read a report that was made by the Department of Justice, which did consultations on the Privacy Act. Between 2020 and 2022, the Department of Justice led engagement efforts with indigenous partners on Privacy Act modernization. This resulted in, among other things, a publication entitled “Privacy Act Modernization: Report on 2022 Engagement with Indigenous Partners”. As of today, in February 2024, a government bill to reform the Privacy Act has not been introduced in the House of Commons.

I have two questions. First, do you think there is an urgent need to reform the Privacy Act, and if so, why? Second, what are the most significant amendments that you would like to see made to the act, based on your reading of the report?

Qujannamiik.

The Chair: Thank you, Ms. Idlout.

Ms. Idlout, I just want to clarify that we want the responses to the questions you asked of the earlier panel to be public, just as we do with these ones. Is that correct?

Ms. Lori Idlout: Yes.

The Chair: Okay. I just needed to clarify that. They'll be going into the digital binder for the committee, but we also want those responses to be made public. Thank you for clarifying that.

That concludes our panel for today.

[*Translation*]

Mr. McIntyre, Mr. Harroun, Ms. Laurin and Mr. Ferron, thank you for your testimony today.

[*English*]

I do have some information for the committee that I want to discuss just briefly. There are a couple of things I need to bring up.

We're expecting the draft report by February 19 on the social media study that we did.

We have confirmation from the President of the Treasury Board, in relation to this study, that she will be appearing March 21. Based on Mr. Green's request the other day, the unions will be appearing on February 15. We've also invited a guest who Mr. Villemure proposed as well. We're still waiting for confirmation on a couple of those. Then, regarding the 137 letters to the various institutions, the email has been drafted. It will be sent out soon, if it hasn't been sent already. The way the clerk is going to gather that information is in a table. It will be distributed to members of the committee as well.

As it stands right now, next Tuesday we'll continue with the next tranche of departmental officials who are to appear. Then, as I said earlier, the unions will be on the 15th. On the 27th, just to remind members of the committee, we have the RCMP commissioner and a staff sergeant, I believe, coming in to speak on SNC-Lavalin.

Without any further business, this meeting is adjourned. Thank you, everyone.