HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

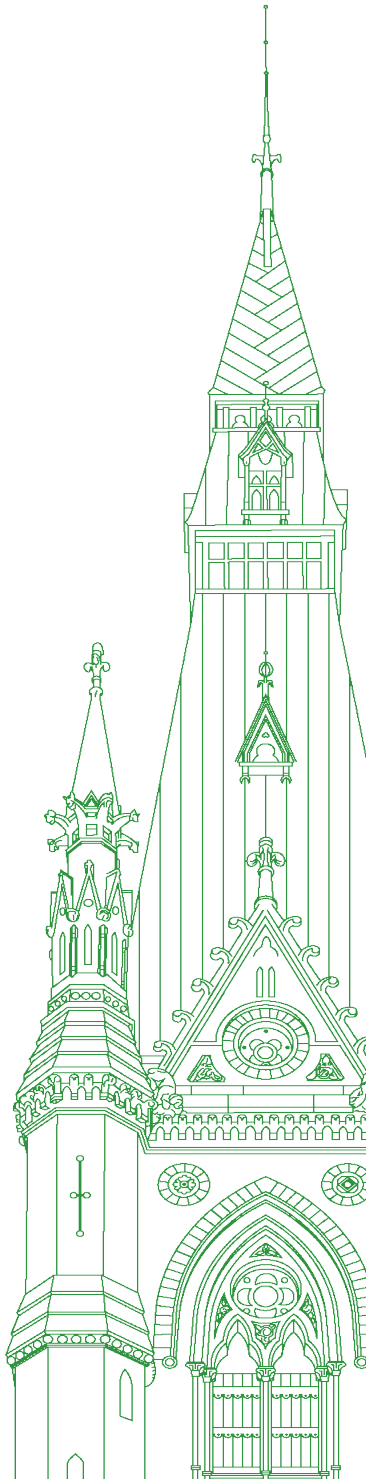
44th PARLIAMENT, 1st SESSION

Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 103

Tuesday, February 13, 2024



Chair: Mr. John Brassard

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, February 13, 2024

● (1130)

[*English*]

The Chair (Mr. John Brassard (Barrie—Innisfil, CPC)): I call this meeting to order.

I'm sorry we're late, but there were votes.

[*Translation*]

Welcome to meeting number 103 of the House of Commons Standing Committee on Access to Information, Privacy and Ethics.

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

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

[*English*]

I just want to remind everyone again, especially our guests, to not put the earpieces next to the microphones, because it could cause feedback for the interpreters. Just be mindful of that.

I would now like to welcome our witnesses for today.

From the Competition Bureau of Canada, we have Pierre-Yves Guay, deputy commissioner, cartels directorate; and Mario Mainville, chief digital officer. From Shared Services Canada, we have Daniel Mills, assistant deputy minister, enterprise IT procurement and corporate services branch; and Scott Jones, president. From the Transportation Safety Board of Canada, we have Luc Casault, director general, corporate services; and Kathy Fox, chair.

Welcome, everyone.

We are going to start with the Competition Bureau of Canada.

You have up to five minutes to address the committee on the subject. Please go ahead.

[*Translation*]

Mr. Mario Mainville (Chief Digital Officer, Competition Bureau Canada): Thank you, Mr. Chair.

Good morning Mr. Chair and members of the Committee. Thank you for the invitation to appear before you today.

My name is Mario Mainville. I am the chief digital officer at the Competition Bureau. Joining me today is my colleague Pierre-Yves Guay, deputy commissioner of the Cartels Directorate.

The Competition Bureau is a law enforcement agency that protects and promotes competition for the benefit of Canadian consumers and businesses. We administer and enforce the Competition Act by investigating and taking action to address anti-competitive business practices that harm consumers, competition and our economy.

We investigate criminal offences such as price fixing, bid rigging and mass marketing fraud as well as civil provisions such as deceptive marketing practices and abuse of market power through restrictive trade practices.

We also review mergers to ensure that they do not substantially harm competition.

Finally, we advocate for procompetitive government policies and regulations.

It is solely within the context of investigations that the Bureau uses the technological tools at issue in the Committee's study.

The targets of these investigations can be sophisticated firms or individuals operating in a deliberately covert or fraudulent manner. Rapidly advancing technology may act as a vehicle permitting users to communicate with others to implement possible anti-competitive conduct and can assist in the perpetration of anti-competitive conduct while acting as a storage device to house information related to anti-competitive activity. In these cases, the Commissioner may apply to the courts for a search warrant in order to gather all necessary information.

● (1135)

[*English*]

It's important to recognize that the Competition Bureau cannot make a decision to search a party's electronic data on its own authority without consent. The bureau must submit a court document setting out the grounds justifying the issuance of the search warrant and the need to search the computer system. The court could then decide to authorize the commissioner to conduct a search of the identified premises and to copy or seize certain records or other things for examination. Our use of these tools is therefore limited by the scope and conditions outlined in these search warrants.

The bureau recognizes the importance of respecting individual privacy rights while executing a search warrant. The issuance of a search warrant by a judicial authority is a safeguard to ensure that searches are conducted with proper legal authorization. Law enforcement agencies are expected to handle and manage the personal information obtained during the investigation responsibly and in accordance with law and constitutional principles. Privacy considerations are relevant, and the bureau has policies and procedures in place to ensure compliance with privacy principles and legal requirements. The bureau works closely with legal counsel from the Department of Justice to ensure that our practices align with both criminal law procedures and privacy obligations. Additionally, any subsequent use, retention and disclosure of information collected during the execution of a search warrant is governed by Government of Canada policies on retention and disposition.

With that, we look forward to discussing these tools with you today. Thank you, and we welcome your questions.

The Chair: Thank you, Mr. Mainville.

Next we go to Shared Services Canada. You have up to five minutes to address the committee. Go ahead, please.

Mr. Scott Jones (President, Shared Services Canada): Mr. Chair and members of the committee, I am very pleased to be here to set the record straight regarding Shared Services Canada's use of technological tools to extract information from government-issued devices.

[*Translation*]

Before I begin, I'd like to acknowledge that we are gathered on the traditional, unceded territory of the Algonquin Anishinaabe people.

With me today from Shared Services Canada is Daniel Mills, Assistant Deputy Minister of Enterprise IT Procurement and Corporate Services.

As you are aware, SSC is responsible for providing the foundational IT infrastructure for the Government of Canada. SSC is committed to improving the digital services that it provides. The department also has a significant role to play in ensuring the security of Government of Canada information while respecting the requirements of the Privacy Act.

[*English*]

Mr. Chair, while the initial media coverage referenced spyware, I want to assure you that under no circumstances is this an accurate description of the tools used by SSC. Departments across the Government of Canada, including Shared Services, use digital forensics tools to support administrative investigations. These tools are essential to our ability to investigate and conclude investigations that I, as deputy head of SSC, am authorized to conduct under the Financial Administration Act.

Investigations happen only when there's a credible allegation of employee wrongdoing and to ensure the security of government networks upon which Canadians depend. Impacted employees are always made aware of the conduct of these investigations, and procedural fairness is ensured. Examples of administrative investigations could include suspected inappropriate website browsing on a government-issued device, malicious software installed on a government-issued device or network, or the unacceptable use of departmental electronic networks and devices, contrary to the policy.

● (1140)

[*Translation*]

Under such circumstances, I have the authority to conduct an investigation and our technical experts need these tools to do their work thoroughly and fairly, while protecting the privacy of employees.

We take the protection of the privacy of employees extremely seriously, and we use digital forensic tools very judiciously.

[*English*]

A security administrative investigation follows very strict standard operating procedures and is taken under the direction of Shared Service's chief security officer. Investigations have a clear mandate and scope, including assurance of independence and impartiality in data collection.

The digital forensics tools used to conduct an administrative investigation are used in tightly controlled environments. Government-issued devices, and only government-issued devices, are brought to a physically segregated secret-level lab, where the tools are then used to conduct analysis: Only information necessary for the investigation is included. In addition, we also use these tools for legitimate operational purposes, such as to accelerate the retrieval of information to respond to requests faster under the Access to Information Act and the Privacy Act.

From a privacy and protection of personal information standpoint, I take the department's responsibility for personal information in SSC's custody very seriously. We have well-established standard operating procedures to protect privacy and embed trust in SSC operations. This is absolutely paramount.

These digital forensics tools are used to analyze large quantities of data and information in digital form. I'd like to add that the Government of Canada has purchased these digital forensics tools for many years. When Shared Services was first created, the purchase of these tools was centralized at SSC to leverage the Government of Canada's buying power and consolidate the number of smaller contracts that were prevalent across the government. As the IT service provider for the Government of Canada, SSC has put in place contracts to acquire these capabilities, allowing other federal departments and agencies to use our contracts to procure them in support of their operations.

[*Translation*]

We are aware that the use of digital forensic tools can raise privacy and ethical concerns. That said, SSC takes the protection of information, the privacy of employees and the security of Canadians very seriously.

I will be very pleased to answer your questions.

Thank you.

The Chair: Thank you, Mr. Jones.

For the next statement, I give the floor to the Transportation Safety Board of Canada.

You have five minutes to address the committee.

[*English*]

Ms. Kathy Fox: Good morning, Mr. Chair and members of the committee.

I would like to thank the committee for inviting the Transportation Safety Board of Canada to appear today.

First, I'd like to take a moment to explain who we are and what we do.

The TSB was created in 1990 by the Canadian Transportation Accident Investigation and Safety Board Act, which contains the act. The TSB is an independent federal agency with a statutory mandate to advance transportation safety by investigating “transportation occurrences” in the federally regulated air, marine, pipeline and rail modes of transportation. “Transportation occurrences” encompass both accidents and situations that, if left unattended, could reasonably lead to accidents.

[*Translation*]

The TSB’s objects are set out in section 7 of the Canadian Transportation Accident Investigation and Safety Board Act. The TSB’s key objectives are to advance Canadian transportation safety by conducting investigations into the causes and contributing factors of transportation occurrences and identifying safety deficiencies, making recommendations to reduce or eliminate any such safety deficiencies and reporting publicly on its investigations and findings.

[*English*]

The TSB has the discretion to investigate any transportation occurrence for the purpose of carrying out these objects. The TSB's policy is to investigate occurrences that have a reasonable potential to result in new lessons learned that can lead to safety actions or that generate a high degree of public concern for transportation safety. The TSB's investigations and its resulting reports highlight issues that federal regulators and the transportation industry must address to reduce risks and safety deficiencies in Canada's transportation system. The TSB is independent and reports to Parliament through the president of the King's Privy Council for Canada.

[*Translation*]

In accordance with its mandate as an investigation and safety agency, the board is not empowered to assign fault or determine civil or criminal liability, and subsection 7(4) of the Canadian Transportation Accident Investigation and Safety Board Act provides that none of its findings are binding on the parties to any legal, disciplinary or other proceedings. TSB is not a regulatory agency and makes no administrative decisions.

● (1145)

[*English*]

Given that we're here today to discuss the use of data, I'd like to touch briefly on our own process for collecting and using data. The CTAISB Act creates a number of privileges and evidentiary rules that are intended to ensure that the TSB has access to the information it requires in the context of its investigations. Pursuant to section 19 of the act, in the context of an investigation, wreckage and other items relevant to the occurrence are collected based on reasonable grounds. These items are examined and tested for the purpose of the investigation. Special tools are often needed to recover pertinent data, which comprises mainly technical information such as any data recorded and displayed in the instrument panel and onboard computers; the position of switches, gauges and actuators; GPS data showing longitude, latitude and altitude; and accelerometer data, which provides the exact position and orientation, as well as information on speed, acceleration and vibration.

Relevant data can include moments prior to and throughout the occurrence.

[*Translation*]

This information is necessary in determining the timeline of a transportation occurrence and enables TSB to fully carry out its mandate. With the exception of audio recordings of, for example, conversations from the flight deck of an aircraft, locomotive or bridge of a ship, pursuant to section 20 of the Canadian Transportation Accident Investigation and Safety Board Act, any items gathered in the context of an investigation are returned to their owner.

[*English*]

As an investigative body, the TSB handles a variety of sensitive information. It is the TSB's top priority and statutory obligation to protect personal information collected in the context of its investigations. For example, the TSB is required to always intervene in court proceedings to protect its privileges, such as witness statements. We are committed to updating our PIAs for our investigation program, to ensure that it is inclusive of all the current technologies used to deliver on our mandate.

The TSB welcomes the opportunity to discuss with the committee how it has always protected personal information in compliance with the CTAISB Act and the Privacy Act.

Thank you.

The Chair: Thank you, Ms. Fox.

For the benefit of the committee, we did get off, obviously, to a late start. I'm going to try to keep it within the timelines. We're going to have time for a first and second round, probably ending up at two and a half minutes. I want to respect the time of members as well, because I know that there are a few of you who have indicated that you have other meetings after this meeting.

We do have to deal with committee business. As I've mentioned, I understand that there is a desire from some members of the committee for a trip. We're on a deadline. We have to submit any request to the Liaison Committee by the 16th, so I need to leave time for some committee business.

We're going to start our first six-minute round. Just for the benefit of the guests, I'm old school. I don't like going through the chair. Deal directly with whoever is asking the questions, and that will be Mr. Kurek for six minutes to start off.

Go ahead.

Mr. Damien Kurek (Battle River—Crowfoot, CPC): Thank you very much, Mr. Chair, and thank you to our witnesses for being here today.

I shared advice with the other witnesses we had before the committee earlier in terms of being proactive about the privacy impact assessments and whatnot. I would encourage all of you, both your superiors and subordinates, to pick up the phone. The Privacy Commissioner has made it very clear that he is happy to engage with you in whatever way possible.

Mr. Jones, because Shared Services Canada is a unique part of how information and technology works across government, I am curious. We've talked a lot about the use of these tools, but I'm a bit curious about the tools themselves. Take emails, for example. If an email is sent from a government device and that email is deleted, is there still a record of it somewhere?

Mr. Scott Jones: From a government device on a government account, the email goes to the server, and there's a record maintained of that email.

Mr. Damien Kurek: Just so that I understand, even if the user of a particular device was to delete it from their phone or their computer, press the trash can and even empty the trash can, would there still be a record somewhere of that email that was sent?

Mr. Scott Jones: There would be. It would be on the server that an email was sent at this time and on this date, and showing the metadata associated with it.

● (1150)

Mr. Damien Kurek: Then it's pretty straightforward, I think, with emails, but are there records of other types of communications—things like phone calls, text messages, accessing the Internet and that sort of thing? Are there similar metadata or specific data that Shared Services would keep?

Mr. Scott Jones: For the mobile phones, it is directly with the telecommunications router, so those records would be retained by the telecommunications provider. I would have to verify if we have access to calls made. To the metadata associated with a call, we definitely don't have access to the calls made. My understanding is no, but I'd have to reconfirm that with our team, just to see if there is some arrangement. We wouldn't have access to the text messages or calls. They would only be on the phone.

Mr. Damien Kurek: When it comes to the data, and we'll go back to emails as the example, it exists somewhere. In terms of being able to access that information for access to information requests, administrative investigations, which you've referred to, that information wouldn't be hidden, even if it's no longer accessible by a government employee, for example? Am I interpreting that correctly?

Mr. Scott Jones: If the email was deleted because it had no records value and wasn't loaded into the official record system—it was deleted from “sent”, etc.—there would still be the record, and anybody who received it would still have a copy of it, but the record that the email was sent would still be in the system logs.

Mr. Damien Kurek: Mr. Jones, the Auditor General, in what was a bombshell investigation just recently, talked about missing documentation for non-competitive contracts. I'm paraphrasing here, but it says that the documentation was missing from initial conversations, so the Auditor General didn't get access to that information, but if emails were sent, it would still exist somewhere in government servers, record-keeping. Is that a fair assumption to make?

Mr. Scott Jones: There should be a record of the “sent”, the fact that an email was sent. What's exactly in that metadata and in that record, we'd have to check. I haven't looked at that for about 20 years in my career.

Mr. Damien Kurek: Okay, but if we were to dig into it, just because the Auditor General didn't have access to this information, if there was information sent from a government server, a government email, it would exist somewhere. You'd be confident of that. Am I...?

Mr. Scott Jones: I would need to verify exactly....

If you're asking if the email itself exists, once it's sent, whoever received it will have a copy of it. Now, whether they delete it or not, the record of the event, that an email was sent, would be in the records.

I'd have to confirm exactly what's stored in that metadata. I just don't know offhand.

Mr. Damien Kurek: Sure. I appreciate this, Mr. Jones, because it's interesting in the context of the fact that the Auditor General was unable to access this information and said that there was missing documentation and whatnot.

Now it would lead one to the inevitable conclusion that maybe tools like what we're discussing here today are required to actually get answers. A cover-up seems to be the obvious conclusion that certainly many Canadians—I being one of them—would jump to in terms of the fact that practices were not followed. It seems like the evidence certainly should be there somewhere.

When it comes to the use of these tools, have you ever been asked to utilize these forensic tools for the purposes of finding information that has been lost from government agencies, departments or independent officers of Parliament?

The Chair: Please give a very quick response.

Mr. Scott Jones: I would have to verify. I can't think of an example in which we've used them in that manner.

Mr. Damien Kurek: Could I ask you to get back to the committee on that?

Mr. Scott Jones: We can certainly do that.

Mr. Damien Kurek: Thank you very much.

The Chair: Thank you, Mr. Kurek.

Mr. Housefather, you have six minutes.

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

I'll come back to the subject that I think we were going to gather here to talk about today, which is whether these tools are taking information and using it in a way that nobody anticipated.

I'll start with Shared Services Canada.

Mr. Jones and Mr. Mills, it's nice to see you again.

Shared Services Canada was created, as I remember it, in 2011. It was created out of different departments. Was the technology at issue in the possession of Shared Services Canada in 2011?

● (1155)

Mr. Scott Jones: The technology we're talking about would have been transferred as part of the amalgamation of the 43, along with the procurement authority to amalgamate those together. We inherited the tools that we're talking about.

Mr. Anthony Housefather: These tools are long-standing. They're not new. You haven't bought them since 2015. They were there before 2015.

Mr. Scott Jones: We've continually renewed the contracts, but those tools were in place during the creation of SSC.

Mr. Anthony Housefather: Perfect.

Are you using those tools to spy on Canadians?

Mr. Scott Jones: Absolutely not.

Mr. Anthony Housefather: Can you advise us on whether there is any mechanism through which you use those tools when the device itself that you're extracting the information from is not in your possession?

Mr. Scott Jones: We don't use those tools in anything other than a physically separate laboratory, where we have the device in our possession. It's a government-issued device, as well.

Mr. Anthony Housefather: Right. Then, when you take the device, are you putting spyware and malware on it so that you can spy on that device afterwards?

Mr. Scott Jones: Absolutely not. Never.

Mr. Anthony Housefather: Are you securing the device only if you have a warrant or if you have the consent of the person involved?

Mr. Scott Jones: When we perform an administrative investigation, we do that with the full knowledge...the person knows there's an administration investigation, but it is a government device, so we do it under that authority from the Financial Administration Act.

These are never the first tools we use, though. We go to these tools only when they're necessary to confirm or disprove allegations that have been made.

Mr. Anthony Housefather: The average Canadian sitting in Winnipeg or Montreal or Vancouver can know with certainty that Shared Services Canada is not spying on their phone right now.

Mr. Scott Jones: Absolutely. That would be completely contrary to our mandate and code.

Mr. Anthony Housefather: Perfect.

Let me ask the same question to the Transportation Safety Board. Can you please assure me that you're not spying on Canadians with the extraction tools we're talking about?

Ms. Kathy Fox: We are absolutely not. We are using the tool in the context of our mandate to conduct our investigations, and primarily with the consent of the owner.

Mr. Anthony Housefather: It would be with consent or presumably a warrant of some type.

Ms. Kathy Fox: We can issue a warrant after a request to a justice of the peace. We've never had to use a warrant for that, because most of the time we get it through consent or on site or through first responders.

Mr. Anthony Housefather: It would be the same in your case, that the extraction process would require you to have the device in your possession. Is that correct?

Ms. Kathy Fox: That's correct. We have the device in our possession. It's downloaded to a stand-alone computer. It's not on a network. It's at our laboratory. It's password-protected as well, as there is very limited access to it.

Mr. Anthony Housefather: You don't download software onto the device. You don't put malware on. You don't put spyware on. You don't put anything on the device that will allow you, after the person resumes having control of the device, to know what they're doing or spy on them in any way.

Ms. Kathy Fox: Absolutely not. We do not keep the information that we download, except for what is absolutely required for the investigation, and we return the device intact to its owner or the owner's representative.

Mr. Anthony Housefather: I imagine in both cases, because I know it's Shared Services Canada but in your case as well, that those who have access to the information are a small, limited group of people who have been properly trained on what they're supposed to do in terms of protecting privacy rights.

Ms. Kathy Fox: That is correct.

Mr. Anthony Housefather: Thank you.

Can I ask the same question of the Competition Bureau, please? Could you respond to the same general questions?

Mr. Mario Mainville: We use the tools in question only with a search warrant that's been authorized by a judge, with the exception of one instance, where there was consent and a consent agreement was drafted. That's only happened one time.

We don't spy on Canadians. We don't install—

[*Translation*]

Mr. Anthony Housefather: I want to make sure I understand.

So, whether I'm in Quebec City, Trois-Rivières, Montreal or Baie-Comeau, you can't see what's on my telephone. The Competition Bureau can't spy on me, can it?

Mr. Mario Mainville: No, we install no software on devices that we seize. In fact, the opposite is true: when we seize a device, we cut all connections and we can't even access the cloud because the information has to be protected. That's part of the procedure. So there's no surveillance activity targeting Canadians.

Mr. Anthony Housefather: I'm going to put the same question to the representatives of Shared Services Canada.

So if you took my telephone because the court issued you a warrant, you wouldn't install any spyware, malware or other program on it to see what I'm doing after I get my phone back.

Mr. Mario Mainville: No, not at all.

Mr. Anthony Housefather: The only way you could look at what's on my phone would be to have the equipment in your possession, at a private laboratory. Is that correct?

Mr. Mario Mainville: Yes, it would be at a lab completely detached from the rest of the Competition Bureau or Government of Canada network.

● (1200)

Mr. Anthony Housefather: That's good.

[*English*]

I will cede back my time, Mr. Chair.

[*Translation*]

The Chair: Thank you, Mr. Housefather.

Since we were talking about Trois-Rivières, I give the floor to Mr. Villemure for six minutes.

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

Good afternoon, everyone, and welcome.

I am glad to have an opportunity to clarify this situation. As you know, we are here today following the publication of the CBC/Radio-Canada article reporting that 13 departments and agencies, including yours, had failed to assess privacy impacts.

So I'm going to put my question to each one of you: have you conducted a privacy impact assessment, yes or no?

Let's start with Mr. Mainville.

Mr. Mario Mainville: No.

Mr. René Villemure: What about you, Mr. Jones?

Mr. Scott Jones: No, but we've created an administrative investigation program, bearing privacy impacts in mind.

Mr. René Villemure: All right, but you haven't conducted a privacy impact assessment.

Mr. Scott Jones: No, we didn't do it any under the program developed when Shared Services Canada was being created. Currently, however, we have begun an assessment.

Mr. René Villemure: I see.

What about TSB, Ms. Fox or Mr. Casault?

Mr. Luc Casault (Director General, Corporate Services, Transportation Safety Board of Canada): We've had an assessment for our program since it was put in place, but we haven't conducted an assessment for the tool itself. Following a conversation with the Office of the Privacy Commissioner of Canada, we decided to update the assessment for our program.

We've been doing this kind of data extraction for a long time. Since an assessment for our program had already been in place for some time, we didn't feel the need to conduct an assessment for the tool itself.

Mr. René Villemure: Did the commissioner recommend that you conduct the assessment for the tool, or was the one done for the program enough?

Mr. Luc Casault: The commissioner definitely recommended updating the assessment for our program.

Mr. René Villemure: Has it been started?

Mr. Luc Casault: Yes.

Mr. René Villemure: All right.

Mr. Mainville, I'm coming to you.

Why didn't you conduct a privacy impact assessment?

Mr. Mario Mainville: Our program was put in place before the privacy impact assessment directive was issued. That doesn't mean that privacy isn't important. When the directive was issued in 2010, we felt that our program hadn't undergone any major changes since it was established in 1996. In 2010, we were already using flip phones and devices in the Nokia and Blackberry lines. Then came smart phones, but we didn't think that adding those new, more advanced devices constituted a radical change to our program.

However, in response to the Privacy Commissioner's testimony and to news that came out in December, we contacted the Office of the Privacy Commissioner and started the process.

Mr. René Villemure: So you started the process for conducting an assessment—

Mr. Mario Mainville: Yes. It was actually for the entire computer forensic program.

Mr. René Villemure: Will there be an assessment for the tool or will it be just an assessment for the program?

Mr. Mario Mainville: From what I understand, the assessment concerns the program and the way personal information is handled. The tool that will be used to do the same work may change, so it's not necessarily the tool that has to undergo an assessment. The recommendation is to proceed with the assessment for an activity or program. In our case, we chose to conduct the higher-level assessment for the computer forensic program.

Mr. René Villemure: The world changed between 1996 and 2010 and between 2010 at 2024. The Internet appeared, along with social media, and now we're able to do new things.

You told us you didn't use those tools without judicial authorization. I understood that, but judicial authorization doesn't replace the privacy impact assessment or the Privacy Commissioner's advice.

In that case, why the delay?

Mr. Mario Mainville: That's a very good question.

I followed all the committee's meetings and noticed that something hadn't yet been mentioned, and that was the jurisprudence issue. During the periods that you mentioned, many cases became precedents, and we had to adjust to that. For example, we had to go and see a judge to have him sign a search warrant. If we had used the same charges as in 2000, he definitely wouldn't have signed the warrant. Consequently, we're forced by the case law to adjust the way we work, to the point where we have to explain to the judge how we're going to handle the information in order to gain his trust so he can sign the search warrant.

So we adjust as the case law evolves. We also attend a number of annual symposia that people from the public and private sectors attend.

● (1205)

Mr. René Villemure: Pardon me for interrupting, but my speaking time is limited.

Do you agree that the case law and the warrant obtained don't replace the privacy impact assessment?

Mr. Mario Mainville: I absolutely agree on that.

Mr. René Villemure: All right.

Mr. Jones, when you requested those tools, you decided to purchase them. So you were the intermediary.

As the tool provider, were you concerned about the need to conduct a privacy impact assessment?

Mr. Scott Jones: Thank you for that question.

The purchase of the tool is one thing; what's most important is how the tool is used. The tool may be used for several purposes. In our case, for example, we use it to retrieve the information we need to meet requests.

Mr. René Villemure: If the Competition Bureau asks you for the tool, Shared Services Canada will purchase it, since that's what the department does. However, Shared Services Canada doesn't worry about what the Competition Bureau does with the tool.

Mr. Scott Jones: No, we don't have—

Mr. René Villemure: That's not your responsibility.

Mr. Scott Jones: No.

Mr. René Villemure: So when you don't have any relations concerning privacy, it's for your own operations.

Mr. Scott Jones: Exactly.

Mr. René Villemure: That's good.

Thank you very much, Mr. Chair.

The Chair: Thank you, Mr. Villemure and Mr. Jones.

[*English*]

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

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

I want to follow up on that and make sure I'm clear.

Mr. Jones, earlier you stated that your department consolidated contracts through whichever other departments would use the technology.

Is that correct?

Mr. Scott Jones: That's correct.

Mr. Matthew Green: In that, you would be responsible for the procurement but not the implementation of the technology.

Is that correct?

Mr. Scott Jones: That is correct.

Mr. Matthew Green: What would be the purchase order line on this type of technology?

Maybe Mr. Mills....

Mr. Scott Jones: We'd have to get back to you.

Typically, what I've seen in the past is that something like this would have a standing offer. We would say, “These are available; we've competed this,” and then it would be a request—

Mr. Matthew Green: We know of 13.

Mr. Mills, I'm going to put this question directly to you.

How many times has this technology been procured through Shared Services?

[*Translation*]

Mr. Daniel Mills (Assistant Deputy Minister, Enterprise IT Procurement and Corporate Services Branch, Shared Services Canada): These tools have been purchased through the Shared Services Canada supply chain since the department has existed. We renew contracts with the various institutions on an annual basis.

[*English*]

Mr. Matthew Green: That wasn't the question I asked. The question I asked was this: How many times has Shared Services contracted this technology out to different departments?

[*Translation*]

Mr. Daniel Mills: We don't have any subcontracting contracts with the other organizations. We procure the services, including technology, which is available to all federal government departments. The departments can use those tools—

[*English*]

Mr. Matthew Green: I'll put the question more directly, sir, and I'm hoping for a direct answer.

You do what you've just described. How many times has this product been accessed and by how many departments?

[*Translation*]

Mr. Daniel Mills: I'll have to check that information and get back to you later.

We purchased licences for tools that can be used by all departments. I don't have a report telling me which department used what tool at what frequency. I don't have that information, but I can check to see if it exists.

[*English*]

Mr. Matthew Green: Okay.

Going back to the contrast between this particular forensic tool and the on-device investigative tools, which we studied here via the RCMP, would the RCMP have had to go through Shared Services in the procurement process, or would they just be direct-to-vendor as well?

Mr. Scott Jones: It would depend. We do provide IT services for the RCMP, but typically anything that's policing action would be directly them through their normal contracting processes or potentially through Public Services and Procurement. I'd have to verify that.

Mr. Matthew Green: Do you have insight or oversight into the procurement practices of other departments?

Mr. Scott Jones: No. It's only when we're doing a shared service and providing the shared licensing where we can get a cost benefit.

Mr. Matthew Green: Okay, that suffices.

Let me just put this question to you: Have you ever, through your work, purchased on-device investigative tools?

Mr. Scott Jones: At Shared Services Canada, no, I can't think of a time in my career when I've done that.

Mr. Matthew Green: Okay. That's important.

Sir, when you were talking about the privacy impact assessments, you had mentioned that your work had predated.... It was going back to 1996. I think you even referenced BlackBerry.

Is it safe to say, though, that you're not using the same technology from 1996?

● (1210)

Mr. Mario Mainville: Yes.

Mr. Matthew Green: You're using new technology.

Mr. Mario Mainville: We're using an evolution of what we used back then, yes.

Mr. Matthew Green: I think it's pretty safe to assume, given Moore's law, that it would be leaps and bounds beyond the technology of 20 years ago.

Is that correct?

Mr. Mario Mainville: Yes, it is, in the ways that we can access the data. Before, it was all or nothing, and now we can actually slice and dice and choose what we see. Yes, it is—

Mr. Matthew Green: Is it much more powerful technology?

Mr. Mario Mainville: Yes.

Mr. Matthew Green: Would it be a material difference from the technology that you would have used in 1996?

Mr. Mario Mainville: We didn't have telephones. These are really in line with telephones, so—

Mr. Matthew Green: It's completely different then if that's the case.

Mr. Mario Mainville: Yes, it would have been computers—

Mr. Matthew Green: It's new technology.

Mr. Mario Mainville: On the actual technology, I would base it more around the arrival of BlackBerrys and flip phones. We did process those in 2009 and 2010.

Mr. Matthew Green: To my point, now, in 2024, we're talking about technology that's an order of magnitude beyond your initial implementation.

The reason I bring that up is that I'm concerned when you say that your program predates the directive, because I interpret a directive from the Treasury Board to be a directive—for all departments. When we have departments picking and choosing when they are under the auspices of a privacy impact assessment....

I'll just go ahead and state that all of this could have been avoided, in my opinion, if these departments had just followed directives and done the PIAs. What we're left with, as a committee, is contemplating what the remedies are, which is to make it a legal requirement of departments.

How would you respond to a question that asks whether making this a legal requirement would provide you with clearer guidelines as to the applicability of the PIA and the use of your technology.

Mr. Mario Mainville: I think the answer is yes, because we worked with newer, substantially modified.... We don't work on an island. We consulted with the Department of Justice on whether our program is modified to the point where we needed a PIA, and we don't.

We make the decision with the information we have, so more clarity....

Mr. Matthew Green: If I could, I think the challenge is that, by allowing each department to opt in or opt out of the PIA, we're creating an unnecessarily conspiratorial outlook on the way in which this stuff is used.

When I hear the explanation about there being a crash and there needing to be a forensic audit of the data, that makes complete sense. There would be a lot of rationale for why you would use this information. I am not here today believing that you're spying on all Canadians or that there's some kind of nefarious thing with this technology.

I believe that to be the case with the on-device, by the way, but that's a whole other conversation.

Pertaining to this study—

The Chair: Mr. Green, you're over.

Mr. Matthew Green: That's okay. I'll have another round.

The Chair: That concludes our first round. We're going to our second round now, starting with five minutes for Mr. Brock.

You'll have two and a half minutes coming up there, Mr. Green.

Mr. Brock, you have five minutes. Go ahead.

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

Good afternoon to the witnesses. Thank you for your attendance. I apologize that I wasn't able to hear the opening statements that, I trust, some of you probably did.

I want to focus on this ArriveCAN scandal that seems to be dominating the House of Commons and Canadians from coast to coast. In following up from my colleague Mr. Kurek, I'm going to focus in on you, Mr. Jones. It appears that you have some expertise in this particular area when it comes to technology, data and things of that nature.

At the heart of the scandal—and this may be news to you—is information. A lingering question the Auditor General laboured with is that, despite all the material she received from the CBSA—which didn't amount to a lot, given the shoddy paperwork and record-keeping—she was unable to determine who chose this two-person firm, which received, essentially, $20 million of taxpayer funds for doing absolutely nothing other than connecting the CBSA with IT professionals.

We have evidence to suggest that information was withheld from the Auditor General, and the information centres around one particular individual by the name of Minh Doan, who happens to be the Government of Canada chief technology officer. One would think, just by having a label of “chief technology officer”, that person would possess the necessary skills to retain records, but at the heart of this, four years' worth of relevant emails—during the pandemic, when the cost of this “arrive scam” scandal ballooned to over $60 million—constituting close to 1,700 emails in total, just mysteriously disappeared.

How can that happen?

● (1215)

Mr. Scott Jones: Without knowing the circumstances, I can come up with a lot of different scenarios in the IT world. It could be as something as simple as—and I've had this happen to me—the hard drive on my laptop failed and I lost my email. Without the specific circumstances, I don't know how to answer your question.

Mr. Larry Brock: That's been a lingering question. He offered no explanation as to why he could not retrieve four years' worth of emails. Despite his status—he was the vice-president of the CBSA at the time, as well as the chief information officer for the CBSA—he was unable to explain that discrepancy, so the CBSA president was unable to really shed any light as to the content—

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

The Chair: Mr. Brock, we have a point of order from Ms. Khalid. I've stopped your time. You have two minutes left.

Go ahead, Ms. Khalid.

Ms. Iqra Khalid: Thanks, Chair.

We're just questioning relevance. I understand that the topic Mr. Brock is highlighting is under study at a number of different committees. We are here on a very specific issue about the surveillance of government employees through government technologies within departments. I would prefer, and I think that the committee would appreciate it, if Mr. Brock stuck to that topic.

The Chair: As I've said in the past, Ms. Khalid, I do give a lot of latitude to members to ask their questions, and I expect that they're going to come back to the topic at hand. I'm certain that Mr. Brock will. He's done it before.

The floor is yours. You have two minutes, Mr. Brock. Go ahead, please.

Mr. Larry Brock: Thank you, Mr. Chair, because I certainly don't frame my questions on the preference of the Liberal Party of Canada. I know they want to shut this down. I know it's important for them to silence us—

Ms. Iqra Khalid: On a point of order, Chair, that is absolutely unreasonable—come on.

The Chair: Thank you for the point of order.

Mr. Brock, please continue. I did stop your time. I'm starting it again. You have a minute and 50 seconds.

Mr. Larry Brock: Thank you.

Mr. Jones, I want to know what tools, potentially, the RCMP, which may be charged with the responsibility of investigating criminality surrounding this arrive scam.... To hearken back to my days as a Crown attorney, what's jumping off the page are allegations of fraud and breach of trust by a public official.

In your professional opinion, sir, what sorts of forensics tools would be available to the RCMP to retrieve four years' worth of relevant emails from the vice-president of the CBSA?

Mr. Scott Jones: I honestly have never been privy to any of the investigative techniques that the RCMP uses. We've always kept them at arm's length, as the IT service provider.

We certainly provide it with base IT—

Mr. Larry Brock: What kinds of tools would you adopt?

For instance, if Erin O'Gorman, the president of the CBSA, actually took her job seriously and wanted to retrieve these emails, what sorts of tools could you adopt?

Mr. Scott Jones: If my colleague was asking for advice, certainly that's what we've established these contracts for in terms of the tooling that's required to retrieve information from government-owned devices. There are a variety of tools, depending on the type of device that would be used.

I don't have a product list in front of me. I've actually never used these tools in my career.

Mr. Larry Brock: Is it possible to retrieve four years' worth of emails?

Mr. Scott Jones: How you'd have to go about that depends on the circumstances and where they are located. It's always very dependent on the circumstances.

Mr. Larry Brock: It's case-specific.

Mr. Scott Jones: Yes, very much.

The Chair: Thank you, Mr. Brock.

Ms. Khalid, go ahead for five minutes.

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

Thanks to the witnesses for being here today.

While the Conservatives try to figure out whether they think surveilling government phones is a good thing or a bad thing based on what they think is good for them for chasing headlines, I think perhaps I'll turn to you.

I would ask you one by one, and I'll start with Mr. Jones.

What do you think is the purpose of a privacy impact assessment and how does that impact the work you do in your department?

● (1220)

Mr. Scott Jones: For me, the privacy impact assessment hits multiple points.

Primarily, it's to ensure we've struck the appropriate balance between the objectives we have to do, for example in the course of an administrative investigation, which is to protect the information and also to follow through on the responsibilities that are conferred upon us by the government with the privacy rights of our employees. As well, it's to make sure we've gone through and done a thorough evaluation to make sure we understand what those implications are, so that we've either put controls in place or we found a way to balance.

Should we need to use a tool that's a bit more invasive than we would like, it's to make sure we've found a balance. For example, that's why we put it in a lab in a secret facility with security-cleared people and very limited access. I can't open the forensics labs, for example. I can't go into it.

Ms. Iqra Khalid: Thanks for that.

The Privacy Commissioner has said that obtaining judicial authorization is not a replacement for privacy impact assessments. In your opening remarks, you talked about the fact that you have to get the warrants before you have those invasive procedures done.

Where do you stand on that?

Mr. Scott Jones: We are not a law enforcement agency, so we have no path to obtain a judicial warrant. My authority is under the Financial Administration Act, as the deputy head, to conduct administrative investigations. Like I said, those are very limited in terms of scope and these tools are used when it's necessary and they're required.

I'll give an example. As Shared Services Canada employees, we do not take our phones out of the country. If the phones or laptops, etc., are taken out of the country, we use these tools to confirm that no documents were taken from the device or that there was no malicious software installed, etc. It's used to confirm our security status and security settings. That's an example of where we'd use these tools.

Ms. Iqra Khalid: Thank you.

Mr. Mainville, I have the same two questions for you, if that's okay with you.

Mr. Mario Mainville: The PIA for a government agency helps us balance our program and our responsibilities to enforce the Competition Act with the privacy needs of Canadians. That's what the PIA is. The primary goal is to systematically assess and proactively address any potential risks associated with new or modified programs.

Ms. Iqra Khalid: Thank you.

Mr. Luc Casault: We agree with the commissioner. It's not a replacement. Obtaining consent does not replace our obligations to have a PIA.

We have had a PIA since the program was created. We have updated it through some of the years. The PIA covers the data we collect. We ensure that all the data we collect is covered in our PIA and assessed against the privacy concerns.

After discussion with the office of the commissioner, we agree with the office that, based on where we're at, it would be a good idea to update that.

The tools don't make for a PIA. Just because you purchase a tool doesn't necessarily change the way you use the data. That's why it wasn't done as a PIA for the tool. However, certainly we believe it is appropriate at this time to update our PIAs, especially with some of the new directions that are coming out from the Treasury Board on this aspect.

Ms. Iqra Khalid: Thank you. I appreciate that.

I'll come back to you, Ms. Fox.

What more can you do to engage with the Privacy Commissioner to ensure that trust in public institutions is maintained, especially when there's intrusive technology on people's phones being employed by the government?

Ms. Kathy Fox: Again, we are not using the tool that was mentioned in the report in any way to interact with employees' phones, government-issued or otherwise. We're only using the tool to extract data under our mandate for the purposes of conducting our investigations, and only the relevant data that we need. The device is returned intact to the owner. Again, we've put this under appropriate security measures in terms of stand-alone computers, limited access and the proper use of retention policies and so on.

We have engaged with the Office of the Privacy Commissioner as recently as last week to just reconfirm our position on this.

● (1225)

Ms. Iqra Khalid: Thank you.

Mr. Jones, I have the same question for you.

The Chair: Give a quick response, please.

Mr. Scott Jones: I actually have met the Privacy Commissioner. It was one of the first things I did when I took over this job, and it was to talk about how we start to look at emerging technologies. This is one of those areas where, frankly, it's a best practice that we should have implemented, and that's why we're doing one now.

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

[*Translation*]

Mr. Villemure, go ahead for two and a half minutes.

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

Mr. Jones, from what I understand, you are new to Shared Services Canada.

Mr. Scott Jones: I've been there since September.

Mr. René Villemure: All right. Thank you very much.

I would now like to go back to Mr. Mainville and follow the same line of thinking as my colleague.

The capacity for action associated with these tools is very different from that of the tools of 1996. You said you didn't conduct a privacy impact assessment in part because there already was an assessment for the program.

Is a privacy impact assessment considered a bit too complicated, unnecessary or a task you can put off until tomorrow? What do you take into consideration?

Mr. Mario Mainville: An assessment was conducted to determine whether we had to conduct a full PIA. During that assessment, we determined that the changes made to the information that we had gathered and to the way it had been handled didn't require a PIA.

As I said earlier, we started the process to request advice on the subject following the Privacy Commissioner's testimony.

Mr. René Villemure: So you stayed in contact with the Privacy Commissioner on this.

Mr. Mario Mainville: Yes.

Mr. René Villemure: The tools used by the RCMP came up in the context of another committee study. I understand we're not talking about the same tools as those we're discussing today, but it was said that it was like when a microphone used to be inserted in the lamp. Honestly, I have to say it's the same thing. I believe that privacy-related expectations are different these days.

You're forging ahead, and I congratulate you on that, but I'm nevertheless disappointed to see that so many departments and agencies haven't done this.

Mr. Mills, earlier my colleague asked you how many departments and agencies had used the tool in question. I would like you to reply to that question in writing so we can make an informed decision.

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

The Chair: You have 30 seconds left.

Mr. René Villemure: That's good.

Ms. Fox, you say you only use this type of tool in an investigation. That's quite specific. Does the fact that it's an investigation release you from the obligation to do a privacy impact assessment?

Ms. Kathy Fox: No. We're required to comply with the Canadian Transportation Accident Investigation and Safety Board Act or the Privacy Act. However, our enabling statute authorizes us to gather information for investigations related to our mandate, but we're also required to protect that information and to use only the information we really need to determine what happened in the incident in question.

Mr. René Villemure: Do those two acts contradict each other?

Ms. Kathy Fox: No, I believe there will always be statutes that grant access to information for specific purposes or mandates, such as transportation safety investigations. If we didn't have access to information, we wouldn't be able to determine what happened or what should be done to prevent an accident. This is a situation in which the public interest is important. We also have to comply with the Privacy Act, but it's a matter of balance.

Mr. René Villemure: Thank you.

The Chair: Thank you, Mr. Villemure and Ms. Fox.

Mr. Green, I'm going to allow you three minutes as well since that's what I gave Mr. Villemure.

[*English*]

Mr. Matthew Green: Thank you.

I'm going to ask all of you the following two questions.

First, in the case where you're using a tool on a mobile device or computer that your employees do access—this is just your opinion—do you think it would be judicious for your institutions to consult the OPC before deploying that use?

Second, would adding a legal obligation in the Privacy Act to conduct PIAs and to submit them to the Office of the Privacy Commissioner of Canada make the process clearer for your institution, and in particular, for government institutions in general—so both your department and all departments?

My asking these questions is not a gotcha. It's to hopefully have a report that provides us with clear recommendations to the government to improve the processes, so you don't have to be here again for these types of scenarios.

Mr. Luc Casault: In terms of using this technology for employees, yes, of course we will consult with the Office of the Privacy Commissioner, as this would be a totally new use. I don't really foresee our ever doing that.

In terms of your second question, I think the better mechanism to get to what we need is more awareness and training of employees, and this committee is doing a good job by actually holding these sessions and bringing that awareness up front. I think the directive is being reviewed. If we can add awareness and training to that, I think it would go a long way, more than—

● (1230)

Mr. Matthew Green: I do have to go on to the other departments. Thank you.

Mr. Scott Jones: From my perspective on the administrative investigation side of things, I think it's important that we continually update our processes, adding in best practices and learnings from other departments and consulting the labour relations experts at Treasury Board. Certainly, having the advice of the Privacy Commissioner there is important in terms of the establishment of the program. We use these tools very rarely in that case.

For the access to information and privacy side, it's important to note that, once these records are under control, this is about us responding to the legal obligation, so we use those very restrictively. However, for example, every once in a while we get a request for all of the text messages sent from my phone. We use this tool to get them—

Mr. Matthew Green: A lot of those requests often come from this committee.

Mr. Scott Jones: —and that makes it quick, because it's very hard. I don't actually.... I can't tell you how to get them off my phone.

Mr. Matthew Green: I appreciate that. I do have to go to the last department.

Mr. Mainville, go ahead.

Mr. Mario Mainville: For your first question, we are a law enforcement agency. We have section 29 of the Competition Act, which requires us to conduct our investigations privately, so that's the beginning of the privacy. It would be very hard for us, on a transactional basis, to go to the commissioner of privacy.

For the second question, yes, I think it would be beneficial if we were all expected to do PIAs on our programs—not specific tools—and then, when those tools change, if they drastically change, to revise the PIAs.

Mr. Matthew Green: We did establish that your tool did drastically change from 1996.

Mr. Mario Mainville: And we are looking at establishing a PIA.

The Chair: Thank you, Mr. Green.

There are two more five-minute question rounds, one each for the Conservatives and the Liberals.

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

Mr. Damien Kurek: Thanks very much, Chair.

To the folks at Shared Services Canada, one of the companies in question here is Cellebrite. I know there are media reports about how the technology can both violate privacy, but also they've had a tech breach. I think it was 1.7 terabytes of data, of information, was made public. One of your big roles is being able to provide, in this case, a very powerful tool.

What processes do you have to make sure that the tools you're procuring actually respect the privacy rights of Canadians, both those that might be used outside the administrative purposes of government, for the purposes of investigations—whether that be agencies we have here or others this committee has heard from—or for administrative purposes, for example, making sure that, for a company that has some pretty serious accusations against it, privacy and rights are protected in that process? What is your process?

Mr. Scott Jones: There are quite a few elements to that question. The first piece is that, when we're procuring, we procure for requirements, so we need a certain capacity or capability to do some aspect. That's what we'll look for. As part of that, there is also a security assessment that's done. We work with our partners at the Communications Security Establishment to ensure supply chain integrity, to make sure that the ownership....

Then lastly, it's how those tools are used and how we deploy them, so for example, any tools like this we use in an isolated lab so that the data stays under our control, in our physical possession and physically isolated as well.

Mr. Damien Kurek: Is that a protocol that you've set up?

Mr. Scott Jones: That last step is for us as a department. How we do the evaluation of the software is a standing process for how we are working with the Communications Security Establishment.

Mr. Damien Kurek: When the article first came out with some revelations and some really serious questions, and a lot of questions.... We've been able to answer a few of those. Again, I'll recommend proactive privacy impact assessments. With respect, all of you operate under acts that were passed by Parliament, and the Privacy Commissioner is an officer of Parliament. Utilize that service, because government is a function of Parliament, not the other way around.

Those are protocols you've created to ensure that this technology is used within that secure room and not connected to the Internet—that sort of thing. Is that what Shared Services Canada has done?

● (1235)

Mr. Scott Jones: That's what we've done in terms of administrative investigations, but for any forensics assessment, yes.

Mr. Damien Kurek: I am curious. There were 13 departments and agencies referenced. Some were no surprise—for example, the TSB and the RCMP—but then there were others where there are outstanding questions and we don't know whether it was for administrative purposes, etc.

Are there any additional departments to the 13 referenced in the article that have utilized the software you have through Shared Services Canada? Are there other departments that would have utilized that software, beyond the 13 referenced in the article?

Mr. Scott Jones: I don't have a list.

I don't know, Dan, if you have seen anything. I don't think so, though.

Mr. Daniel Mills: I don't think so, but as I mentioned earlier, we can provide the committee with a list of all departments that have used it, if they are in addition to the 13 that were listed in the article.

Mr. Damien Kurek: I think there are two very distinct things. There is the administrative side of things, ensuring that employees' rights are protected and whatnot, and then there is the investigative side of things, whether it's because of an airplane crash or a competition circumstance, as in the case of our other guest here.

If you could delineate the difference between those circumstances, where it was used for administrative purposes versus for investigative purposes, I think that would be very helpful.

Further, it would be nice to know about judicial authorization, but I suspect that probably goes beyond the mandate of what Shared Services would be able to provide. Am I correct in that assumption?

Mr. Scott Jones: I don't think we would know the purpose of the tool, other than making a guess at the mandate. We can certainly look at which departments or agencies have procured through us, but we wouldn't know what purpose they were using it for.

For example, the RCMP is not going to tell me what tools they use in a police investigation.

Mr. Damien Kurek: You're the IT service providers, so you're not going to get answers. If you could provide that information and if you know about both the administrative purposes and investigative purposes, that would be very helpful for us to answer what are the still serious outstanding questions that I think many Canadians have.

The Chair: Thank you.

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

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

Thank you to everybody for joining us today. My first question is for the Competition Bureau.

You indicated some of the duties that you perform. You talked about bid rigging, price-fixing and things like that. You investigate those things.

Would these tools be used in an investigation of that manner?

Mr. Mario Mainville: Yes.

Mr. Parm Bains: If you're trying to combat price-fixing, bid rigging or those kinds of things, as a law enforcement agency, you would target someone of interest and then you would still need to get the judicial consent to go after and investigate them and then use these tools to do your work.

Mr. Mario Mainville: That is correct.

Mr. Parm Bains: In Canada, I think we have a challenge with oligopolies. We have, for example, groceries and telecoms that we look at, and ultimately this small group of large companies pretty much controls the market. For example, with respect to grocers, we even heard in the House of Commons that if a certain person were in charge of grocery prices or something, those prices could come down.

Would that be something you could look at?

Mr. Mario Mainville: I'm going to turn to my colleague, Pierre-Yves.

Mr. Pierre-Yves Guay (Deputy Commissioner, Cartels Directorate , Competition Bureau Canada): It is certainly an allegation that we can look into. That's for sure.

Mr. Parm Bains: A complaint would come forward and so on. What would be the process that you would go through?

Mr. Pierre-Yves Guay: Our processes are very similar to what the police could do in terms of an investigation. It could be that one of your constituents could complain to us, for example, and bring us some information. If we have enough information to pursue, we will start using our own tools in terms of investigations—searches, for example—if we have the grounds to do them. Let's say that we seize a cellphone from one of the targets. Then these tools would be used.

● (1240)

Mr. Parm Bains: Then from the cellphone, what can you extract?

We saw some demonstrations in previous meetings here. You would need to obtain the phone, connect to it and extract everything they have. Is that right? Would you have access to all the apps and everything in there?

Mr. Mario Mainville: We would have access to everything that's in the phone. What we'd be interested in, in the case of bid rigging, is whether that individual has communicated with somebody from the other company to set prices—those types of communications.

As has been mentioned a lot in the study so far, we do have processes where only relevant information makes it to the case files. If you see me as the forensic person, I would only give information to my colleague Pierre-Yves, who is the investigator, that is relevant to his file. He would not get the whole address book unless he had reason to believe.... It would be really restricted to what was outlined in the search warrant.

Mr. Parm Bains: The search warrant would have to be very specific, pinpointed, and then only he would have access to it.

How many people in your department have access to all of this? How many investigative people are there?

Mr. Mario Mainville: Initially, when we come back from a search, the number of people who have access to the images of these telephones would be eight to 10, depending on our complement at the time. Right now, there are eight forensic practitioners.

Only the relevant data would then be made available to the case team, and only the case team. Similar to other law enforcement agencies who have testified, this is not made available to all of the cartels directorate. It's made available to the case team investigating that one matter.

Mr. Parm Bains: Then you would be alerted if somebody else were to come in and look at that information. You have those mechanisms in place.

Mr. Mario Mainville: The computer forensics is what I've heard called an “air gap network”, so it does not connect to any other network, not to the Internet. It is within a secured room, inside a secured room, with restricted physical access.

The Chair: You just went over your time there, Mr. Bains.

Mr. Parm Bains: Thank you.

Thank you very much.

The Chair: Thank you, Mr. Bains.

I want to thank our guests for being here today.

There have been some requests to undertake to send some information to the committee. The clerk is going to follow up with you, but I would like that information in the hands of the clerk by five o'clock next Tuesday, if possible. That is a week from today. As I said, the clerk is going to follow up.

I want to thank all of you for being here today. I am going to dismiss you. We have some committee business that we need to discuss.

Thank you so much.

On the committee business, members, I understand there is an interest in taking up an offer from the RCMP to have a technical briefing in their facilities.

Mr. Motz, is that something you would be interested in as a former RCMP officer?

Mr. Glen Motz (Medicine Hat—Cardston—Warner, CPC): Absolutely.

The Chair: There are two options that we have here. We can make a formal request, which means that we have a deadline of the 16th to make that request to the Liaison Committee for approval.

The other option we have is to make an informal visit to the RCMP, which I understand is the desire of the members. I want to make sure that the circumstances of that are clear. Any informal visit to the RCMP to discuss the issue of privacy collection, etc., cannot and will not make it into the report. There's nothing that can come from that and make it into the study. It's just as a matter of interest for the committee.

Ms. Damoff, I see your hand—and Mr. Brock.

Is there anyone else?

Go ahead, Ms. Damoff, on this issue.

Ms. Pam Damoff (Oakville North—Burlington, Lib.): Thank you, Chair.

I did have a conversation with Bryan Larkin after the last meeting and with Michael Barrett, who is not here right now. However, with the public safety committee—and Glen, I think went—we went to the gun vault in an unofficial capacity, just to learn more about the issue. I think Bryan has offered to educate us more on privacy and cellphones and what they're able and not able to do.

My concern is that, if we go with a formal process, Chair, it takes quite some time, assuming it even gets approved. It could be June before we get approval to go. At that point, we'll have already finished the study and moved on to other issues, so I'm happy to coordinate this with the other four parties.

It's here in Ottawa, so it doesn't require transportation. The RCMP is able to conduct these tours in the two official languages, so we don't get into issues of not having access in French.

That would be our recommendation, Chair. I'm happy to coordinate it with Michael and the others.

● (1245)

The Chair: Thank you, Ms. Damoff.

Just for the benefit of the committee, the headquarters is in Orleans, so it's not too far away.

Mr. Brock, your hand was up, and then we'll have Mr. Kurek.

Mr. Larry Brock: I wanted clarification of the site, and that's been answered.

I wholeheartedly agree with Ms. Damoff. That's the right approach to take.

The Chair: Thank you.

Go ahead, Mr. Kurek.

Mr. Damien Kurek: Thanks.

I had a quick chat with Michael, and I understand that there have been some discussions here. I think informal is certainly best, and it doesn't have to cost taxpayers a penny. We can do this.

I would just note on the record as well that, if there was information that became relevant to the study, I think it would be entirely appropriate for us to request that the RCMP provide it in a follow-up. Although the tour itself wouldn't necessarily be on the record, certainly the information that we learn could be included in that future report. I appreciate that the RCMP has extended this opportunity for us to help understand these tools.

The Chair: Thank you, Mr. Kurek.

I'm sensing that there is consensus among us for this to be an informal trip.

[*Translation*]

Mr. Villemure, go ahead.

Mr. René Villemure: Mr. Chair, I would like to officially introduce the following motion, notice of which I gave last week:

> That, pursuant to Standing Order 108(3)(h), the committee undertake a study of misinformation and disinformation and their impact on the work of parliamentarians, that the committee devote the next three available meetings to this study, that the committee invite experts in the field of misinformation and disinformation and that the committee report its observations and recommendations to the House.

The Chair: Your motion is admissible, since you previously gave the committee notice of it.

Would you like to say something about the motion, Mr. Villemure?

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

In reading prospective studies, one sees that, among the concerns of current leaders and governments, misinformation and disinformation now present a risk almost as great as climate change.

In Parliament, we have to make informed decisions. Consequently, we too are likely the target of misinformation and disinformation. So to assist the committee and Parliament in making more informed decisions, I invite us to conduct this study together with experts on the basis of the public interest. This will help us move forward and enable all concerned parliamentarians to do a better job.

The Chair: Thank you, Mr. Villemure.

I just want to clarify one point, since the committee's business has already been established and we are starting a study that we have already decided to take.

If I correctly understand you, Mr. Villemure, the study you propose would be conducted during future meetings. Is that in fact the case?

Mr. René Villemure: Yes.

The Chair: All right.

[*English*]

Next I have Ms. Khalid followed by Mr. Green.

I see your hand, Mr. Barrett.

Go ahead, Ms. Khalid.

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

Through you, I'd really like to thank Monsieur Villemure for bringing this motion forward. I sit on the Commonwealth Parliamentary Association as vice-chair. In our discussions amongst Commonwealth countries, this is the number one issue amongst parliamentarians across the world. How do we deal with misinformation and disinformation? How does it impact our democratic institutions? How does it impact how we make decisions?

I 100% agree with Monsieur Villemure as to how important this issue is. I would hope that we would spend a little bit more time than just three meetings on this. I think we need to do a deep dive into how we can make sure that governments are prepared for the changing face of technologies, for the changing face of digital media, and how it impacts the spread of information and misinformation and disinformation. I can come up with at least 10 witnesses on this issue who I think would be great contributors in terms of coming up with recommendations on how we as the Canadian government can deal with this issue, not only to provide safety and security for Canadians in the information they are absorbing at such a fast rate nowadays but also to ensure that the information we are taking in is accurate, honest and objective and is not nefarious in its objectives, as well.

I would really appreciate it if, with the consensus of the committee, we could say “at least” three meetings on this. After those three meetings, we could come back to it and see how many more witnesses we have who would be interested to speak to this and how much more information or areas within this topic we need to dive into a little bit deeper. We could re-evaluate where we would like to go with this study.

I really congratulate Monsieur Villemure for bringing up this very important topic. I think we really need to do that deep dive. I would friendlily propose that we say “at least” three meetings and re-evaluate at the end of those three meetings.

Thanks, Chair.

● (1250)

The Chair: I'll take that as a formal amendment. It's difficult to amend motions on a friendly basis.

I'll take that as a formal amendment and seek consensus on the change Ms. Khalid is proposing, that we have “at least three” meetings rather than “three”.

We're still on the amendment, if anybody wants to speak to it.

Go ahead, Mr. Barrett, on the amendment that would change “three” meetings to “at least three”.

Mr. Michael Barrett (Leeds—Grenville—Thousand Islands and Rideau Lakes, CPC): Yes. Three's fine. I just wanted clarification also on the motion that's being amended.

Is it the understanding that as it's worded—

The Chair: The motion says, “next three available meetings”. We do have meetings scheduled, which I will touch on after we dispose of this, but “next three available” is what Monsieur Villemure is proposing.

I'll seek consensus on the amendment, if there's no further discussion.

(Amendment agreed to)

The Chair: We're now back to the main motion as amended.

Mr. Green, go ahead.

Mr. Matthew Green: Thank you.

Again, I appreciate the good work of my friend from the Bloc, René Villemure, for setting the course of our next study.

I'm just going to put my cards on the table and say that I am satisfied with the outcomes of the study we're currently in. I get a sense that we could ask eight more departments and get very similar answers. I am satisfied that this is not on-device information technology or spyware or malware. I am satisfied that it is used within the regulations of the respective mandates of the departments for investigative tools and for audit tools. I'm satisfied with the parameters in which they're using it. I'm not satisfied with the lack of the PIA, which I've expressed.

Having said all that, Mr. Chair, how many more meetings were scheduled for that particular study? Would it benefit the committee to perhaps move a motion to direct the analyst to begin a draft report on the work we've done on it to date?

The Chair: I was going to update you. This is perfect timing.

We have one more meeting on this. You expressed a desire to have the unions come in and discuss this in terms of the public service. We've arranged to have the Canadian Association of Professional Employees and the Professional Institute of the Public Service of Canada come in on Thursday. Unfortunately, PSAC has declined to come in.

Those witnesses are coming in. One witness that Monsieur Villemure wanted to see was the source of the CBC/Radio-Canada article. He is coming in on Thursday as well. Thank you for reminding me of this. The President of the Treasury Board has committed to March 21. That will effectively tie this study closed. That's where we're at.

● (1255)

Mr. Matthew Green: I guess my next question would be when the next three available dates would be.

The Chair: The only thing I can see right now would probably be February 29 as the start of this particular motion, if it does get passed. On February 27, we have the commissioner of the RCMP coming in on SNC-Lavalin.

Just give me a second.

The clerk just reminded me again. I was talking to Alexandra about this. We have the RCMP commissioner coming in on February 27, and then we have the draft report on the social media study that will be available by February 19. As it stands right now, I'm calculating probably up to three meetings on that. It could be less. I'm hoping it'll be less. There are a few recommendations there.

Hang on there, Damien. I'm on a roll here.

That's where we stand right now. There are the unions and Mr. Villemure's guest on Thursday, the break week, the RCMP commissioner on February 27 and, on February 29, I anticipate that we're going to start the draft report on the social media study. Then, on March 21, it's the President of the Treasury Board.

It's not likely that we're going to get to this. We have break weeks in the month of March as well. We may not get to this until we're back from the majority of those break weeks. Is that okay? Good.

Damien.

Mr. Damien Kurek: You answered my question.

Ms. Iqra Khalid: You answered my question as well.

The Chair: That's why I was on a roll. The only problem is that I didn't do it in French, René, and I'm sorry.

Mr. René Villemure: Well, Damien was interrupting.

The Chair: Rudely.... He was rudely interrupting.

Some hon. members: Oh, oh!

The Chair: We are on the main motion as amended. Is there consensus on the main motion as amended, or do we want to go to a vote? Are we fine?

(Motion as amended agreed to)

[*Translation*]

The Chair: Thank you for introducing that motion, Mr. Villemure.

I had—

[*English*]

Mr. Michael Barrett: Mr. Chair, it's national Kindness Week. I would just like to make note of that.

As the House of Commons sponsor for national Kindness Week, I would just like to take this moment to wish everyone a happy national Kindness Week. With this motion passing unanimously, it's a good sign of the wonderful possibility of our great country.

The Chair: Let me interpret that for you: Mr. Barrett will be proposing a motion at some point.

Some hon. members: Oh, oh!

The Chair: I don't know when that's going to happen, but he's going to look for the same type of kindness.

I don't see any other business.

Thank you to the clerk, analysts and technicians.

I'm going to adjourn this meeting. We'll see all of you on Thursday.