HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

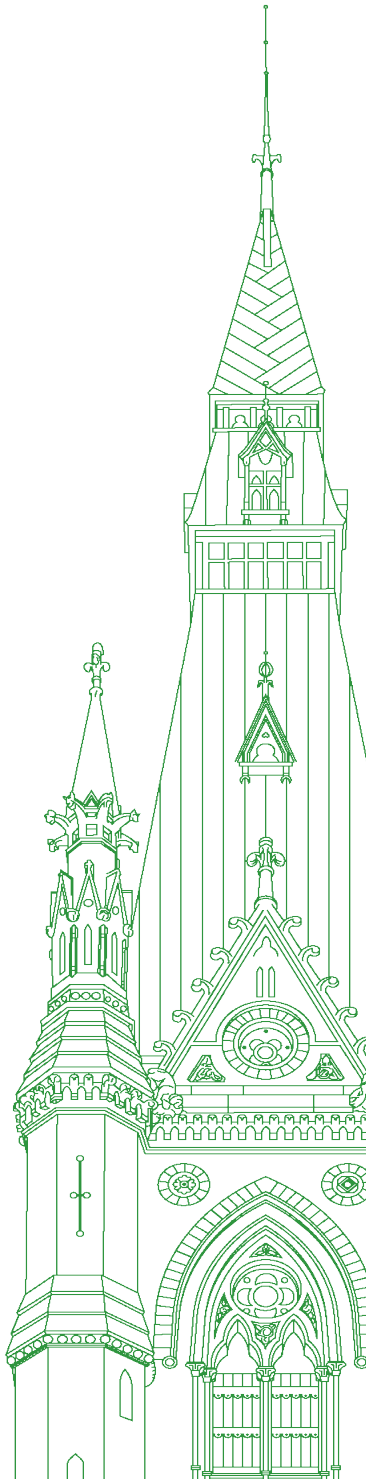
44th PARLIAMENT, 1st SESSION

Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 100

Thursday, February 1, 2024



Chair: Mr. John Brassard

Standing Committee on Access to Information, Privacy and Ethics

Thursday, February 1, 2024

● (1100)

[*English*]

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

[*Translation*]

Welcome to meeting No. 100 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 commencing today its study of the federal government's use of technological tools capable of extracting personal data from mobile devices and computers.

[*English*]

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.

I just want to remind all members again not to put the earpieces next to the microphone as it causes feedback and could cause potential injury to our interpreters.

I'd now like to welcome our witnesses today. From the Offices of the Information and Privacy Commissioners of Canada, we have Mr. Philippe Dufresne, the Privacy Commissioner of Canada. Welcome, sir. We also have Lara Ives, executive director of the policy, research and parliamentary affairs directorate.

Before Mr. Dufresne begins, he has asked for up to 10 minutes to address the committee. I've granted that.

The other thing I will remind members of is that since we have only these two witnesses for the next two hours, we will reset the clock at the top of the hour and give Mr. Villemure and Mr. Green the additional time that they need.

Mr. Dufresne, again, welcome, sir. It's good to have you at the committee, as always.

Please commence with your opening remarks.

Mr. Philippe Dufresne (Privacy Commissioner of Canada, Offices of the Information and Privacy Commissioners of Canada): Thank you, Mr. Chair and members of the committee, for the invitation to contribute to your study on the federal government's use of technological tools capable of extracting personal data from mobile devices and computers.

Last fall, CBC/Radio-Canada reported that 13 federal institutions had acquired such tools. The media reports raised questions about the reasons for their use and whether these organizations were respecting their privacy obligations in using the tools.

Initial reports referred to them as covert surveillance or spyware. Since then, it has been clarified that the tools are digital forensic tools, which are distinct from spyware. Digital forensic tools are used to extract and examine large numbers of files from laptops, hard drives or mobile devices. They are typically used in investigations or technical analysis, and often with the knowledge of the device owner.

[*Translation*]

They can be used to analyze the metadata of a file, or to create a timeline of events, such as when an account was used, when websites were accessed, or to see when an operating system was changed. These tools can also be used to recover deleted data or to ensure that data has been properly wiped from a device before it is discarded or repurposed. This makes them useful investigative tools that can help to preserve the integrity of an evidence chain.

Digital forensics tools are distinct from spyware in that spyware is typically installed remotely on a person's device without their knowledge. It can then covertly collect personal information, such as keylogging and web-browsing history. One example would be on-device investigative tools, or ODITs, which are used by law enforcement to obtain data covertly and remotely from targeted devices. Importantly, in the context of law enforcement, judicial authorization is required prior to their use.

● (1105)

[*English*]

In August 2022, I testified before this committee as part of your study about the use of ODITs by the RCMP. You will recall that in that case, the RCMP advised the House that it had been using ODITs in recent years to obtain data covertly and remotely from targeted devices, but had not completed a privacy impact assessment, or PIA, and had not advised my office.

In my appearance at the time, I noted that PIAs were required under Treasury Board policy, but were not a legally binding requirement under privacy legislation. I recommended that the preparation of PIAs should be made a legal obligation for the government under the Privacy Act.

[*Translation*]

In its November 2022 report, the committee endorsed this recommendation and also called for an amendment to the preamble of the Privacy Act to indicate that privacy is a fundamental right, and for the act to be amended to include the concept of privacy by design and explicit transparency obligations for government institutions. I welcomed and supported these recommendations, and the committee may wish to reiterate them as they remain outstanding and relevant.

[*English*]

With technology increasingly changing the manner in which personal information is collected, used and disclosed, it continues to be important that government institutions carefully consider and assess the privacy implications of their activities to determine if and when PIAs are required.

My vision for privacy is one where privacy is treated as a fundamental right, where privacy supports the public interest and innovation, and where Canadians trust that their institutions are protecting their personal information. Conducting a PIA and consulting my office before a privacy-impactful new technology is used would strengthen privacy, support the public interest and generate trust. This is why it should be a legal obligation for government institutions under the Privacy Act.

[*Translation*]

Currently, the Treasury Board Secretariat's directive on privacy impact assessment requires that institutions conduct PIAs when personal information may be used as part of a decision-making process that directly affects an individual; when there are major changes to existing programs or activities where personal information may be used for an administrative purpose; when there are major changes to existing programs or activities as a result of contracting out or transferring programs or activities to another level of government or to the private sector; and when new or substantially modified programs or activities will have an impact on overall privacy, even where no decisions are made about individuals.

[*English*]

In our advisory discussions with federal institutions, we promote the use of PIAs as an effective risk management process. PIAs ensure that potential privacy risks are identified and mitigated, ideally at the front end, across programs and services that collect and use personal information. That said, the use of a new tool does not always trigger the need for a PIA. This will depend on how the tool is being used and what is being done with the information that it collects.

The OPC has used digital forensic tools, for instance, in the context of certain breach investigations to determine the nature, scale and scope of the incident, including how a breach occurred and what types of personal information, if any, may have been compromised.

[*Translation*]

Digital forensics tools, however, can be used in ways that do raise important risks for privacy that would merit a full privacy impact assessment.

For example, when conducting an internal investigation about an employee's conduct where a decision will be made that will directly impact that individual, or as a tool used as part of an inquiry into alleged criminal activity.

In those types of cases, a privacy impact assessment would be required—addressing not only the specific tool being used to collect personal information, but the broader program under which the tool is being used.

● (1110)

[*English*]

It is incumbent on all federal institutions to review their programs and activities accordingly. Where digital forensic tools are used in the context of employee monitoring, institutions must take steps to ensure respect for the fundamental right to privacy and foster transparency and trust in the workplace. There should be clear rules about when and how monitoring technologies are to be used. My office updated its guidance on privacy in the workplace in May 2023, and my provincial and territorial colleagues and I issued a joint resolution on employee privacy in October 2023.

In the present case, following the CBC/Radio-Canada reports regarding the use of digital forensic tools in the federal government, my office followed up with the institutions that were listed there and in this committee's motion to proceed with this study.

[*Translation*]

To summarize what we learned, three organizations indicated that they had completed and submitted a privacy impact assessment—or PIA—on the relevant program; one organization indicated that it had procured the tool but never used it; another organization indicated that a PIA was not required; and the remaining eight organizations indicated that they had either started work on a new PIA, or were considering whether to conduct a new PIA or to update an existing one in light of their use of the tools.

[*English*]

We will continue to follow up with institutions to insist that PIAs be completed in cases where they are required under the Treasury Board policy, but without a requirement in the Privacy Act there are limits to what we can do to ensure compliance. Privacy impact assessments, in appropriate cases, are good for privacy, good for the public interest and they generate trust. In this increasingly digital world, they should be a requirement under privacy law.

I'd be happy to take your questions.

The Chair: Thank you, Mr. Dufresne. It is well under time, and I appreciate that.

We're going to start with our first round of questioning.

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

Mr. Michael Barrett (Leeds—Grenville—Thousand Islands and Rideau Lakes, CPC): Good morning.

Do Canadians have a right to privacy?

Mr. Philippe Dufresne: Absolutely.

Mr. Michael Barrett: Can you give us examples of the software that's been used by the Government of Canada to spy on Canadians?

Mr. Philippe Dufresne: As I've described, these types of digital forensic tools are able to retrieve information from devices, from computers, to see information that may have been deleted or not deleted. They are able to obtain information, including personal information, which is why in situations where they're used and directed toward individuals, whether it's employees or in other circumstances affecting their privacy, a privacy impact assessment should be done.

Mr. Michael Barrett: Can the software that the government is using unlock a locked smart phone?

Mr. Philippe Dufresne: My understanding is that they could in certain instances.

Mr. Michael Barrett: Can it access password-protected laptops and iPads?

Mr. Philippe Dufresne: My understanding is that it can. These questions should be asked of the institutions as well.

Mr. Michael Barrett: In terms of the personal information that could be accessed, can you give us an idea of what the range of that personal information would include?

Mr. Philippe Dufresne: Personal information could be the data that's contained on this: information, the files that are on that device and other types of use, whether something was deleted or not deleted or whether a website was accessed. These are tools that have important capabilities. That is why, in situations where they're being used to target individuals or to investigate individuals, this is where we would expect to see privacy impact assessments being conducted, so that these things can be assessed and mitigated.

Mr. Michael Barrett: Photos, text messages, direct messages, search history—they're all accessible using these tools.

Mr. Philippe Dufresne: Our understanding is that they could be—absolutely.

Mr. Michael Barrett: Can the tools being employed by the government track the movement of Canadians?

Mr. Philippe Dufresne: Track the movement of Canadians...?

Mr. Michael Barrett: That's their physical location in real time or their physical location history.

Mr. Philippe Dufresne: Typically, these types of devices will not be used remotely with the device not being in the possession of the investigator. You would have that device in your possession. That was one of the distinctions between those and the on-device, the ODITs, or the spyware, where you can access the device with the individual not knowing that you have it and not being in possession of the device.

● (1115)

Mr. Michael Barrett: Let's be clear: The spyware being used, once the device is in the possession of the government, can retrieve information, even deleted information, but there are remote capabilities as well where software can be covertly installed and then used to track the location and the use of a device.

Mr. Philippe Dufresne: If we're talking about digital forensic tools, which is what we're talking about in this context, they can be used to acquire digital evidence, recover deleted files, analyze files of interest and create a timeline of interests and events. They almost always require the physical access to the device.

That's the distinction between what is spyware or ODITs, where you could do that remotely, without the knowledge of the individuals. They're different tools, but they still nonetheless have important capabilities.

Mr. Michael Barrett: How many government departments have this capability?

Mr. Philippe Dufresne: I don't know of all the departments that would have it, but certainly from the reporting, 13 were identified as having those tools. We followed up with them and have obtained information.

Mr. Michael Barrett: Is the only way that you or your office would be aware of the intention to use, or that a department had, this capability is if government departments were each individually required to complete a PIA, a privacy impact assessment, in advance?

Mr. Philippe Dufresne: In many cases that's correct, because we don't know what a department is doing unless they advise us or unless they consult us. The policy of the Treasury Board requires it, but it's not a legal obligation. My recommendation is that it should be. It is always better for the department, for Canadians and for my office when that proactive reach-out is done from the department so that we can provide our input, we can flag risks and Canadians can see that this is happening.

Some of these tools can be used appropriately—there are good reasons for it—but we need that privacy check. We need that assessment.

Mr. Michael Barrett: Do you differentiate between the types of tools that government departments use when you consider something like the COVID app, where the government said they wouldn't use the app to track the movement of Canadians, but that's exactly what they did? It seems like the government attitude toward the right to privacy that Canadians have is lacking.

Mr. Philippe Dufresne: I think we have to strengthen that generally. More and more technology is being used with greater capabilities. That brings innovation and that brings opportunities, but we need to have that reflex of privacy by design and privacy at the front end. Often we'll see the situation where the tool is developed and used, and then we do a privacy impact assessment or we bring in those things.

It will always be more economical and more prudent to bring privacy at the front end. It's more important than ever in this day and age, when we have AI and we have technology that is ever more capable. We really recommend that this be a legal obligation for that purpose.

The Chair: Thank you, Mr. Barrett and Mr. Dufresne.

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

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

Thank you to our witnesses for being here today.

To clarify a couple of points that were pointed out by Mr. Barrett, these digital forensic tools are specific to employees within these departments. Is that correct?

Mr. Philippe Dufresne: In the cases where they're used for administrative investigation, these are not the only purposes. Some departments would use them for other types of investigations, but certainly if we're talking about administrative investigations, that would be the employees of the department.

Ms. Iqra Khalid: To be clear, is it all Canadians and all their devices that these departments are investigating or keeping an eye on, or are we talking specifically about government devices provided to government employees as they're conducting their work within our government?

Mr. Philippe Dufresne: We're talking about a range. Some of the departments will be using them to do investigations on breaches of the act by Canadians generally. Others will be using them to investigate their employees. In the case of the three that were using them for administrative investigations, that won't be all Canadians. It will be only their employees.

However, employees also have privacy rights. There are obligations. We've issued that guidance: Make sure your tool is used for a purpose that's linked to the one you've identified. Make sure it's transparent. Make sure it's proportional. Make sure you conduct a privacy impact assessment where appropriate.

● (1120)

Ms. Iqra Khalid: Right.

Are we talking about accessing employees' devices, the ones that are provided by the departments, or are we talking about their personal devices where these digital forensic tools are being installed?

Mr. Philippe Dufresne: I don't have all the details of what they would be doing. That could be asked of them.

Generally speaking, you would be talking about the tools that are provided to the employee by the employer—the email, the laptop and these types of things. Again, nonetheless, there are some expectations of privacy vis-à-vis these tools, but it's contextual. Employers have legitimate reasons for obtaining certain types of information. We talk about that in our guidance and really highlight it: Make sure you've assessed the tool. Make sure you've assessed the necessity and proportionality of it. Make sure you are transparent about it and people know.

In our annual report last year, we talked about one of our investigations in the private sector where a trucking company was using a monitoring device for truck drivers. Even when they were not on duty, they were being filmed and recorded 24-7. We found that this was too broad. It was legitimate to do it when you were driving, for safety reasons, but it had to be limited to that. That was done.

This is the type of questioning that goes on with regard to the privacy impact assessment. When my office is consulted, especially before it's initiated, then we can raise these types of questions. Let's prevent these things. Let's prevent Canadians worrying about it so that they can feel like, “Okay, this is a tool and here's what it does. The Privacy Commissioner's office was consulted and provided input.”

That's what I'd like to see more of, especially in situations where we often learn after the fact that something was being used.

Ms. Iqra Khalid: I do find it concerning that this directive was not followed. Has there been any contact with these departments by you or by your office, either initiated by you or by these departments?

As well, you spoke about it being a policy of TBS. Can you just highlight the distinction between policy and a mandated process for privacy by design, especially in these departments?

Mr. Philippe Dufresne: The policy is an internal rule that the government imposes on itself, so it's a directive that would be issued, in this case, by the Treasury Board. It says, here are the expectations that we have of the department. It's certainly important but it doesn't have the same binding legal force, and it certainly doesn't allow me to conduct an investigation in the same way as if it were in the Privacy Act. That's why I'd recommend, and the office has recommended, to make it a legal obligation. I've recommended this for the private sector as well, especially vis-à-vis AI because I compare this to predeparture flight checks in airplanes. It's something that will bring comfort and reassurance when we're using powerful tools.

In instances like this we've reached out to the departments. We have regular consultation with departments, and we have a government advisory team that's always on standby to hear consultation from departments. Again, what we see sometimes is, “Okay, we will now do a PIA. We will now update it, and we have a program.” Sometimes we're told that this is authorized under their program legal authorities, or they are doing it under a warrant. We have to remind those departments that, even if you're doing it under a warrant or under a valid legal authority, the privacy impact assessment is a separate question. You may still need to do that if your legal use of that tool nonetheless impacts the privacy of Canadians.

It's an extra step, and if it were a legal obligation my belief is that we would see more compliance up front rather than situations like this, where sometimes people find out about it through important media reports. Again, it may well be that these tools are appropriate for their purposes. They're distinct from spyware. They're distinct from ODITs. Even ODITs in appropriate cases may be acceptable, but having that discipline and having those PIAs seen to be done builds on that trust that Canadians can have to say, “Okay, I don't have to watch over my shoulder constantly. The institutions themselves have these tools and these reflexes.”

Ms. Iqra Khalid: Can you distinguish the difference between spyware and ODITs, as you just mentioned that.

Mr. Philippe Dufresne: Generally, when we talk about spyware we're talking about these types of tools that will be covertly accessing phones, retrieving data, turning on cameras and turning on recordings. It's the broad category of spyware we recently referenced for illegal use and unauthorized use. When we talk about ODITs, on-device investigative tools, we're talking about those types of things that are used by law enforcement authorities. They're similar tools, but when they're used by law enforcement authorities, with legal authorization and with judicial warrants, it's appropriate and it's legal. Nonetheless, as a law enforcement authority, you also have to do a PIA before doing those things.

● (1125)

Ms. Iqra Khalid: I just have one last question, Mr. Chair. It's very short.

The Chair: You're six minutes and 38 seconds into it.

I'm going to go to Mr. Villemure, and you'll have another opportunity in another round.

[*Translation*]

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

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

Mr. Dufresne, welcome back to the committee. We're always happy to see you again.

Were you surprised when you heard the news that 13 departments and agencies were using these kinds of tools?

Mr. Philippe Dufresne: What I would have liked, in a situation like this, is for my office to have been consulted beforehand in the 13 cases and for us to have all the necessary information so that, in response to the media, we could confirm to them what has happened, tell them that we have been notified, that we have given advice, that an assessment has been made and that we have no problem with it, or the opposite, and then present the recommendations we have made.

The surprise is that we finally have to follow up with the departments to find out what's going on.

Mr. René Villemure: So the surprise is to learn that people don't necessarily have the reflex to consult the commissioner in this kind of situation.

Do departments and agencies have a good understanding of the Privacy Act or their privacy obligations?

Mr. Philippe Dufresne: I think there are all kinds of challenges, whether in terms of resources or the pressure on departments. They're in a better position to speak to that than I am.

The challenge is that privacy impact assessments are mandatory under the Treasury Board directive but not under the act. The directive makes distinctions, for example, between a new program and the update of a program, or between the assessment of a program and the assessment of the tool itself.

Given these distinctions, the department can say in good faith that it is of the opinion that an assessment isn't required, because the directive doesn't require it. And yet, perhaps it should be required. With technology becoming increasingly powerful, it could become even more important to reassure Canadians that we're doing all this in an even more proactive manner. So it would be preferable that it be a legal obligation.

Moreover, this is not an issue that concerns only Canada, obviously. My international colleagues, at the conference of the Global Privacy Assembly, adopted a resolution on artificial intelligence in the area of employment. It calls on governments and parliamentarians to be aware of the need to set guidelines. If artificial intelligence technologies are used to recruit workers and assess their performance, that can have an impact on privacy. So we have to be transparent and take into account the notions of necessity and proportionality. These are fundamental questions.

Mr. René Villemure: In its current form, the Privacy Act does not require departments and agencies to be exemplary when it comes to privacy. We've already discussed this.

Mr. Philippe Dufresne: This isn't a legal obligation for them, which would become a top priority. It's only an obligation under the directive.

Mr. René Villemure: Rest assured that we'll do everything we can to ensure that it's included.

When I saw the list of 13 departments and agencies, I was surprised to see how much it covered. It wasn't just the policing agencies, such as the RCMP, the police, or Correctional Services.

Are we talking about glibness, laziness, negligence or mistakes? You talked about a lack of resources. However, when it comes to privacy, especially if it's considered a fundamental right, a lack of resources isn't an acceptable answer. Do these people treat privacy in an offhanded way?

Mr. Philippe Dufresne: Before setting up a program, they don't always have the reflex to check whether my office has been informed of it. There are improvements to be made in that regard. We're talking about departments that use this tool for a specific purpose: Some use it for internal investigations and others for investigations within their mandate.

The use isn't necessarily inappropriate per se, but that assessment has to be done. However, as we've seen, people sometimes say that they don't need to do that assessment because their legal mandate includes authorization to carry out those activities. My message to the departments is that it isn't enough. The privacy impact assessment is a separate topic that needs to be dealt with more proactively.

Mr. René Villemure: A little earlier, you talked about proportionality. That's a concern I have. Sometimes you can get the result you want by using a less intrusive method, but we've seen in other areas that the most intrusive method is used, not because it's intrusive but simply because it's faster.

Is this proportionality included somewhere, in a directive, or would it be desirable to include it eventually in an act?

● (1130)

Mr. Philippe Dufresne: In terms of the public sector, again, this notion of proportionality is not included in the Privacy Act. We recommended, and this committee did as well, that the issue of necessity and proportionality be included. At this point, it is more a Treasury Board directive that this use is necessary to achieve the desired objective.

Currently, the act requires that the use be related to a mandate of the organization. For our part, at the Office of the Commissioner, we will implement that necessity and proportionality by raising questions about it in our investigations. We're talking about it now, just as we talked about it during the investigations into the measures taken during the pandemic, in particular. When we talk about this, though, we have to recognize at the outset that this is not a legal obligation and that, if it were not respected in a given situation, it wouldn't be a violation of the act.

This is a very important recommendation. The approach is very similar to how we proceed in the context of the Canadian Charter of Rights and Freedoms to determine whether there is discrimination or a violation of fundamental rights. We determine whether the objective sought is important, whether the proposed measure achieves the objective, whether the method used to achieve it is the least intrusive and, lastly, whether the method is proportional.

You're absolutely right: We may be tempted to use a tool because we find it very efficient and quick. Artificial intelligence comes to mind. Yes, it's effective, but we're talking about a fundamental right here.

Having said that, it's not an either-or. Personally, I'm in favour of technology. In the office, we have made it one of our three strategic priorities recently. We want to use technology, but in a way that protects privacy. In that sense, the privacy impact assessment tools are essential. These assessments must not only be done, but also be seen to be done.

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

[*English*]

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

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

You know, I'm thinking back to the work that we conducted on the RCMP, and my hope is that, at the time, these departments may have been tuned in, knowing that they were actively engaged in similar activities. My disappointment is that it took them this long to kind of come clean. There are 13 departments. Certainly, there are many more federal departments, some that may or may not be declared. I won't impugn what the other departments are doing.

I do note that in the language of the directive on privacy impact assessment, in paragraph 3.3, it states that the Privacy Act requires "assessing the privacy implications of new or substantially modified programs and activities involving personal information". I believe you just referenced this, sir. Then the next line says, "However, if not properly framed within an institution's broader risk management framework, conducting a PIA can be a resource-intensive exercise."

How resource-intensive is it?

Mr. Philippe Dufresne: It requires the discipline. It requires that you look into your program, that you answer some questions. That's why they're not going to be required in all cases. It's legitimate that there are criteria. They are not so resource-intensive that they're not worth doing.

Mr. Matthew Green: It seemed like a weird condition to me. In the language of a directive to put that "However" and associate it with resources. Given what I think we've determined at this committee in terms of the importance of democracy and the importance of our privacy, it seems like a weird one. That's my opinion; it's not yours.

I think you said that the Treasury Board encourages PIAs. I would put to you that under section 5.1, the Treasury Board directive specifies that PIAs are conducted on "new or substantially modified programs".

If it's under the language of a directive, in your opinion—I'm just asking for your opinion—a directive is different from encouragement. Is it not?

Mr. Philippe Dufresne: I would say yes.

Mr. Matthew Green: Is it fair to say, then, that the Treasury Board doesn't encourage...? They actually, in fact, through the directive, specify that this should happen.

Mr. Philippe Dufresne: I agree.

Mr. Matthew Green: Given that this is section 5.1 of the directive on the Privacy Act and these departments did not...is it fair to say, on the face of it, that they were in breach of section 5.1 of the Treasury Board's directive?

Mr. Philippe Dufresne: A number of the departments, in this instance, that have not done those PIAs are not compliant with this directive.

● (1135)

Mr. Matthew Green: Presumably there are others, at this point, that we might not have knowledge of. When you look at section 5.2.1 of the directive, you see that it provides that "PIAs are conducted in a manner that is commensurate with the level of privacy risk identified prior to establishing any new or substantially modified program". Not only are they derelict in their application of a PIA, but the fact that they even started the program without the PIA.... Based on my reading of this subsection, it states that they're in a pretty considerable breach.

Mr. Philippe Dufresne: Yes, there's that element of "do it before the fact, not after the fact".

Mr. Matthew Green: However, that's a directive.

Mr. Philippe Dufresne: That's the directive.

Mr. Matthew Green: It's not an encouragement.

Mr. Philippe Dufresne: That's correct.

Mr. Matthew Green: However, these agencies went ahead and did it anyway.

In that, I think there's an important distinction to make, because I don't want Canadians to leave feeling like the federal government has this ability on all devices across the country. We certainly studied, to our chagrin, the use of movement-tracking technologies over the course of COVID. I think we did a pretty good job of unpacking that. In this case, this is for federal employees, and if I'm to understand your testimony, those who are under investigation of being in contravention of the act.

Is that correct?

Mr. Philippe Dufresne: Yes.

Mr. Matthew Green: When we look at Fisheries and Oceans, CRTC, Environment and Climate Change, the Competition Bureau, the CBSA, RCMP, National Defence, it could include civilians. Is that correct?

Mr. Philippe Dufresne: Yes.

Mr. Matthew Green: In the case of its including civilians, I would assume, based on your testimony, that this technology needing to be in the possession of government.... Would that require a warrant?

Mr. Philippe Dufresne: In some cases it would. In some cases it wouldn't. In a situation where you're doing an internal investigation of employees, it wouldn't.

Mr. Matthew Green: However, for civilians, for instance....?

Mr. Philippe Dufresne: In many instances you would need a warrant in those cases. The departments have indicated that. As was the case for the study on the RCMP's use of ODITs, those also require warrants. However, that's a separate question from the privacy impact assessment. The warrant may be based on criteria that are distinct from the privacy considerations that are at the heart of the privacy impact assessment.

Mr. Matthew Green: I am concerned that there wasn't a definitive "yes, they would need warrants when applied to civilians."

In what situations would it be the case that warrants would not be needed for civilians who are not federally employed?

Mr. Philippe Dufresne: That's a question that would be best placed to the specific department, because it's their use of their—

Mr. Matthew Green: That's fair enough.

In your assessment or investigation of this, would that be a consideration that you would consider? Would they be required to report to you about instances where there was no warrant and no PIA?

Mr. Philippe Dufresne: The warrant issue is relevant to us when we're looking at the legal basis for the use. That's one criteria. One investigation that we did years ago involved the use of cell towers. Some of the things were done without a warrant, and we said that's not justified.

Mr. Matthew Green: Do you mean the Stingray technology, specifically?

Mr. Philippe Dufresne: I think so. We'll get the exact name.

That was an issue. We looked at that as the first question. Even if you have that warrant, and you have that legal basis, there is then the second question: Do you have to do a PIA?

Mr. Matthew Green: Just in summary, for the privacy impact assessment, you are putting that as something that would be a consideration on top of a warrant. Even for something that might be legal by basis of a warrant, that might not be ethical or in keeping with the act, in your opinion, under a PIA.

If you determined, under a PIA, that it wasn't those things, do you have the power to actually stop them from implementing these technologies?

Mr. Philippe Dufresne: I don't because it's not a legal requirement. We can flag it and Treasury Board can raise it, but it is all internal to the government's rules.

Mr. Matthew Green: Thank you.

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

That completes our first round of questioning. We're going to go to our second round now.

You know how much I hate interrupting on a timeline. We went well over the six minutes on each of the rounds, just to be fair to everyone. Let's try to keep it a little bit tighter now to the five minutes or whatever time we have. We're getting into the meat of the issue here, I believe, and I want everybody to have that opportunity.

Go ahead, Mr. Kurek, for five minutes, please.

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

Thank you, Commissioner, for being here. Thank you to your team for their work.

I just want to highlight something for those listening and watching. There are 13 government institutions that were called into question in the article that's been mentioned. It's Fisheries and Oceans Canada, Environment and Climate Change Canada, the CRTC, the CRA, Shared Services Canada, the Competition Bureau, Global Affairs, the Transportation Safety Board of Canada, Natural Resources Canada, Correctional Service Canada, the Canada Border Services Agency, National Defence and the RCMP.

I think, like many Canadians, that some of those are not surprising. I think it's disappointing that they did not conduct PIAs, as was referenced. The question around trust is certainly highlighted here.

Commissioner, do you believe that this information would have come to light had it not been reported? Is there a reporting mechanism within government that would have said, these tools are used and here's the number of times? Had it not been for this article that references this, would this information have come to light otherwise?

● (1140)

Mr. Philippe Dufresne: We were not aware of all of those uses. We were aware of some of the programs, but that's the issue the directive on the privacy impact assessment is meant to address. We should be advised. My office should be advised before these new tools and activities are deployed.

Mr. Damien Kurek: I'm hopeful that we'll have a minister sitting in the chair that you're in at some point.

Does your office have the resources to ensure that there are timely responses to the PIA questions that would be asked by any of these 13 departments?

I'm quite frankly concerned that there may be more than this. If we have 13 departments and they work with a lot of other departments...and on and on the story goes.

Are you confident that your office would be able to respond and give advice as needed, whether it's to these 13 or other departments that may be utilizing tools like this?

Mr. Philippe Dufresne: Generally, I have asked for more resources from Parliament for my office, including for our promotion activities. We do have a government advisory team that is on standby to provide advice to departments. We prioritize what we get based on the importance and impact. We will continue to monitor that. We may be making more requests for additional resources.

Certainly, the key thing is that we need to know about those matters. We need to be advised by the departments prior to these things happening. That's also part of the policy directive of the Treasury Board.

That's what I'd like to see more often, more proactive reaching out from those departments to say, “We're considering this. Do we need a PIA? Here's the information.” That's so we don't find out about it in the media. The media reporting is very important in this case, but ideally, this would be something that we would have known in advance.

Mr. Damien Kurek: Just to clarify, if somebody called you, even if it was a developing situation that required a level of immediacy, somebody would be there to pick up the phone and you'd be able to provide advice and a response. That's just to clarify.

Mr. Philippe Dufresne: Absolutely. We're there for that. We give advice. We flag issues. We're not there to be a roadblock to innovation and the public interest. We're there to provide advice and to say, “This is the privacy implication and this is how you should address it.” We provide more transparency. That's good for everyone.

Mr. Damien Kurek: I appreciate that, because quite often we hear that it was urgent so they didn't have the time or they didn't have the resources. I appreciate your clarifying that here today.

Of those 13 departments, have any PIAs been completed since this time?

Mr. Philippe Dufresne: Three of the departments have finalized the PIA on the relevant programs. That's been done. On the others, one of them had purchased the tool and didn't use it—so there's no PIA—and the majority, eight of them, are going to be updating or doing a new PIA. That is all outstanding.

Mr. Damien Kurek: When it comes to the question that was asked as to who this applies to.... It's not widespread, like Mr. Green and Ms. Khalid had mentioned. It's not everybody in the country, but certainly there are some instances where it is the employees of a department. That doesn't diminish privacy expectations, as we've talked about, but there are instances where there may be citizens, where there are not warrants, who have been subject to these materials being used.

I just want absolute clarity in the last few seconds here that I'm interpreting what you've said correctly.

Mr. Philippe Dufresne: I'm saying that I'm relying on the departments to comply with their legal obligations in terms of whether a warrant is required or not, and their authorities.

What I'm flagging is that they have to conduct privacy impact assessments. In a number of cases here, they have not.

The Chair: Thank you, Mr. Kurek and Mr. Dufresne.

Mr. Bains, I have you next for five minutes. Go ahead, sir.

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

Thank you to the commissioner and our witnesses for joining us today.

Commissioner, has your office begun investigating any of these departments as a result of these revelations?

● (1145)

Mr. Philippe Dufresne: I think I heard the question to be whether we have investigated any of those departments as a result of this. We have not. As indicated, it's not a legal requirement under the Privacy Act, so I would not have a basis for investigating noncompliance with that directive. We have reached out to them and we're going to continue to do so. We're going to continue to insist that PIAs have to be conducted.

My recommendation to this committee and to the House is that it should be a legal obligation in the Privacy Act. It should also be a legal obligation in the private sector privacy act, so that this becomes a proactive duty that would then give me a clearer mandate and authority to make sure that it's done. Canadians would see that this is part of their privacy protections.

Too often Canadians will feel that they're left to their own devices. It's up to them to consent. It's up to them to inform themselves. We do give tips to Canadians on best privacy practices and so on, but Canadians deserve to feel that their institutions are there to protect them and for them to rely on, knowing that government is using this, that government has consulted the Privacy Commissioner's office and that there are privacy experts who are in on this from the design.

That's what I want to see more of. That starts with an obligation in the Privacy Act.

Mr. Parm Bains: Part of our job here is to generate recommendations. The main recommendation of yours is to make it a requirement to do so.

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

Do federal institutions make a clear distinction between a new and an existing program or activity?

Mr. Philippe Dufresne: They do. That's where sometimes you'll have an interpretation that this is not a new program, that this is an existing program and that they haven't really changed what they're doing; they just have a new, more powerful tool. They didn't do a privacy impact assessment on that tool because the program was already assessed. That type of situation may well be consistent with the policy in the sense that the directive would not require a new privacy impact assessment in that case.

It does raise the question, when we're talking about very powerful tools—perhaps it's not a new program but if it changes it so much now that you have this capability—of whether Canadians would benefit from more transparency on that new tool, even if it's within the same program.

Mr. Parm Bains: Should any other changes be made to the Treasury Board directive on the PIA? What other things could be changed?

Mr. Philippe Dufresne: What I would like to see is more proactive reach-outs to my office in terms of new initiatives. We have that requirement in the policy, but we are not seeing that happening in most instances.

I think it's that reflex of saying, "You're not going to move forward on this until you've had that consultation, you've had that reach-out and you've done that due diligence," and perhaps also clarifying that, in instances where a tool is much more powerful, it may require a second look at an existing program.

Mr. Parm Bains: You've made these requests. What are the next steps after today as it relates to these 13 departments?

Mr. Philippe Dufresne: From our standpoint, we're going to continue to reach out to those departments. We're going to follow up to insist that the PIAs be completed where they have not been. We're going to continue to ask questions and work collaboratively with them.

I hope, as part of this committee's work and as part of the legislative process, that we see a modernization of the Privacy Act. I'd hope that the modernization includes a legal obligation to conduct PIAs in appropriate cases and also other elements like necessity and proportionality, which we have discussed. There's an opportunity for that.

Currently, the House is seized with private sector law reform. We hope to see that move forward with appropriate changes, but the Privacy Act is even older legislation. I really hope to see that come before the House soon.

● (1150)

The Chair: Thank you, Mr. Bains.

Thank you, Mr. Dufresne.

[*Translation*]

Go ahead, Mr. Villemure. You have two and a half minutes.

Mr. René Villemure: The Privacy Act dates back to 1983, doesn't it?

Is the proactiveness you're referring to here something that should be included in an act? Is that going to make it easier?

Mr. Philippe Dufresne: I think when you have a statutory obligation, it emphasizes that obligation; that's always the case. It is indeed much easier to fall back on a directive or a policy, but an act really imposes pressure, constraints, the need to take the time, and to manage the situation differently.

The act should require that relevant details be provided to the Office of the Commissioner within a prescribed period of time before a program is established. Those details can be set out either in the act or in regulations. That proactiveness is important.

Mr. René Villemure: Obviously, in 1983, it was perhaps not as urgent.

Would Law 25 in Quebec have prevented that kind of surveillance?

Mr. Philippe Dufresne: I know that Law 25 includes certain requirements for privacy impact assessments, particularly when data leaves Quebec or is related to the use of new data by the government or the private sector. The act has certainly codified the need for such assessments in some cases, but I would have to get back to you with details on that.

Mr. René Villemure: In the context of a possible review of the Privacy Act, are there any lessons from Law 25 that we could learn?

Mr. Philippe Dufresne: Law 25 gave the Commission d'accès à l'information du Québec the power to issue orders and the ability to impose administrative monetary penalties. It may be less essential in the public sector context, but it can still help treat privacy as a fundamental right and make it a priority.

I think that, both for the private sector and for the public sector, we can certainly draw inspiration from comparable elements, including Law 25.

Mr. René Villemure: I'm going at random here, but surely the act, as it was written in 1983, doesn't have any provisions dealing with artificial intelligence, does it?

Mr. Philippe Dufresne: That's for sure. The act was written before the advent of the Internet and social media. There have been a lot of changes that mean that the laws have to be modernized.

That said, I would like to take this opportunity to repeat that my colleagues, both in Canada and internationally, and I have made a number of statements on AI indicating that existing laws apply. They may not have factored in AI, but they are technologically neutral. We certainly interpret them as applying to artificial intelligence. We have ongoing complaints about that. We issued a joint statement on that. We work very closely with our provincial and territorial counterparts.

There's no doubt that modernizing these acts would clarify certain things, particularly this aspect of proactiveness. I specifically recommended it with respect to AI in the context of modernizing the private sector legislation. Among other things, we're talking about algorithmic assessments, and we're talking about all that, because it's very important.

The idea isn't to reject the technology, but to set parameters.

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

I gave Mr. Dufresne more time so he could finish answering the question.

[*English*]

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

Mr. Matthew Green: Thank you so much, Mr. Chair.

Looking at this, I think you referenced an important term when you talked about obligations under the Privacy Act and Canadians relying on institutions. Ultimately, would you agree that privacy is about trust?

Mr. Philippe Dufresne: I agree.

Mr. Matthew Green: In that trust, we're looking at scenarios for our federal employees in a world where, increasingly, your cellphone is a reflection of almost every aspect of your life, whether it's your mobility or.... I think about the apps I have on my phone. I have health tracking apps and different things that are deeply personal to me. As a federal employee.... I think even about the watch I'm wearing, for instance, and the heartbeat. It tracks everything—finances and absolutely everything.

We've talked a lot about the technological aspects and context of this technology. We haven't spoken about the human context, which is ultimately on the other side. There's somebody who has access to this.

In your work, do you review who, precisely, has access to the information? Is there a level of clearance or security, or is this a mid-level IT guy who might want to check to see if I have pictures of or text messages to somebody they may or may not like?

Mr. Philippe Dufresne: That's a very relevant consideration in terms of management of information generally, as well as in terms of a privacy impact assessment. It's looking not only at what are you obtaining and why, and whether you need it, but also at how you are protecting it.

We're seeing more and more situations of privacy breaches, cyber-attacks and information being stolen, so the security of that information is very important and who has access and the need to know—

● (1155)

Mr. Matthew Green: Directly to the point, in the PIA is there a consideration for the level of clearance required to view what ultimately could be deeply personal information?

Mr. Philippe Dufresne: There is. There is a consideration of the retention practice and the safeguard practices. That would go to—

Mr. Matthew Green: In your experience, who would have access to this information within the IT frameworks of these departments? What level of responsibility would they be given?

Mr. Philippe Dufresne: They would be best placed to answer that question, but certainly at the OPC we look at the information: What type of information is it? Is it protected A, B or C? Are there security risks to individuals if this is lost? Are there national security considerations?

There's a whole range of rules and criteria that have to be followed to protect. It's going to be—

Mr. Matthew Green: I have a last question. Have you had any complaints, subsequent to this story breaking, from employees or the union based on the use of this technology? Have there been any complaints to your commission?

The Chair: Please give a quick response.

Mr. Philippe Dufresne: We have not received complaints on this that I'm aware of.

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

We'll go to Mr. Brock for five minutes and then to Mr. Erskine-Smith.

We haven't done a test on Mr. Erskine-Smith. We'll see how that goes when he starts, and then we'll reset for six minutes after that.

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

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

I'd like to thank the witnesses for their attendance today. This is a very important and serious issue for not only Canadians but also the public service. I want to start by looking at some legal principles.

Every Canadian, and that includes every public service employee, has an absolute right under the Canadian Charter of Rights and Freedoms to be secure against unreasonable search and seizure, pursuant to section 8. Although you've testified, sir, that in some cases legal authorization was obtained, you can't say for certain that in all cases authorization was obtained. That raises charter considerations. A breach of a section 8 right is a serious violation that, hearkening back to my years as a Crown prosecutor, quite often was not met with success. There are strict consequences for the privacy rights of Canadians as upheld by courts across this country.

That backdrop was important for me to frame this question. When I look at the 13 institutions that were identified, there's no guarantee that these are the only 13 institutions that have been using this technology. Is that a fair assessment, sir?

Mr. Philippe Dufresne: That's fair.

Mr. Larry Brock: Yes...because these are the institutions that were identified by the CBC reporter. Is that correct?

Mr. Philippe Dufresne: Yes.

Mr. Larry Brock: When I take a look at this list, I might give some consideration to Fisheries and Oceans Canada, and perhaps the Competition Bureau, but when I take a look at Canada Revenue Agency, Global Affairs, Correctional Services, Canada Border Services Agency, National Defence and, most importantly, the RCMP, they all have great legal teams working behind them—in many cases the Department of Justice—who would certainly instruct not only management of those departments but its employees about the protection of privacy rights. To learn, then, that in many instances judicial authorization was not authorized, that a PIA was not submitted for your consideration and that data was collected, raises serious privacy concerns.

You mentioned earlier, sir, I think in your opening statement, that in many cases when this device was used on public sector employees it was with the consent of the device owner, but you can't say that in all cases the extraction of data pursuant to this software already had the consent of the device holder. Is that fair to say, sir?

Mr. Philippe Dufresne: That's fair. I don't know that for certain.

Mr. Larry Brock: Right—which again raises more privacy breaches.

The RCMP said after the fact that they submitted a PIA, I believe in December. Is that correct? Some organizations said they submitted it perhaps earlier. Can you tell us whether or not you have consulted with these departments that have not submitted the PIAs and asked them specifically why they circumvented the Treasury Board directive in these circumstances?

● (1200)

Mr. Philippe Dufresne: We reached out to all 13 organizations. As I indicated at the outset, three of them indicated that they have done a PIA on their program. The remaining ones have not. We're going to be reaching out to all of them. We're going to continue that exchange to follow up and say, “Okay, we want to understand when this is going to be done and why it wasn't done and make sure it's done in the way that it needs to be done.” However, we don't have legal authority to compel that if there's no agreement.

Mr. Larry Brock: That is something that could be enhanced with an amendment to the Privacy Act. Is that correct?

Mr. Philippe Dufresne: That's right. That's what I'm recommending.

Mr. Larry Brock: As the Privacy Act is constructed, not surprisingly, there are no legal consequences or any penalties for noncompliance with the PIA requirements. Is that fair, sir?

Mr. Philippe Dufresne: That's fair. In my office I don't have order-making powers, even for things that are in the Privacy Act. I can do an investigation and make a finding, but I have to rely on the government or the institution complying with that.

Mr. Larry Brock: Is that something that perhaps you would recommend as a possible amendment as well, sir?

Mr. Philippe Dufresne: Yes, I would, certainly.

Mr. Larry Brock: Thank you.

The Chair: Thank you, Mr. Brock.

[*Translation*]

Thank you, Mr. Dufresne.

[*English*]

Mr. Erskine-Smith, you have five minutes. We're going to make sure that your technology is working. Go ahead.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Thanks, John. It's nice to see you.

It's nice to see everyone here, especially the analysts.

Commissioner, have any of the 10 of the 13 departments that have not yet done PIAs refused to do one?

Mr. Philippe Dufresne: One of them has indicated that they purchased the tool and never used it. They did not indicate they were going to do one. One indicated that in their view it wasn't required. We're going to be following up to see if we agree with that and have a discussion.

Mr. Nathaniel Erskine-Smith: Which one said that it wasn't required?

Mr. Philippe Dufresne: It was the Competition Bureau.

Mr. Nathaniel Erskine-Smith: Okay.

In terms of the other ones, it would be helpful if you put a timeline on them of, say, 20 to 30 days. Then you could refer back to us and let us know if you haven't had a response, because you may not have powers, but we obviously do have powers to compel attendance.

On the instances, you have one department reply to say they've never used it. What's the scale of use here, depending upon the department? Do you have a sense of how often this tool has been used?

Mr. Philippe Dufresne: We have various answers. For some of them it seems to be more regular as part of their activities. Some have indicated a smaller number of uses. For our standpoint, whether it's used two, three or four times or whether it's used regularly, we look at it in the same way. Is it appropriate, and should they do the PIA or not?

Mr. Nathaniel Erskine-Smith: Let's pull that apart.

Obviously they should do a PIA. I can't imagine anyone here disagreeing that they should do a privacy impact assessment. I take your point. It's well stated. There should be an obligation in law that these organizations, when they're using a new tool with impacts upon privacy, do a PIA.

Let's talk about appropriate use, though. In the CBC report, I saw an indication from agencies and departments that they use this tool separate to judicial authorization in some cases, and in other cases only on government-owned devices and in cases involving employees suspected of harassment.

Both of those instances, at a high level, sound quite reasonable to me. Are there other instances that you're aware of that we ought to be concerned about?

Mr. Philippe Dufresne: I saw the departments' responses. They've provided information about the types of programs they would use this for. There hasn't been anything that has worried me in terms of this being a completely inappropriate purpose or use. They're using this to fulfill their mandates as organizations, to apply their enabling legislation or to do some investigation.

What I'm concerned about is this: Has the privacy consideration been done well, was it done in time and have the risks been mitigated? Obviously, that's my purview. Specific questions about the legitimate authority they have or their mandates would be distinct and perhaps things this committee can ask.

My concern at this stage is that we need to consider the privacy impact in all situations where you can impact the privacy of Canadians. That's not always been done.

● (1205)

Mr. Nathaniel Erskine-Smith: I know you're getting back to the need for a privacy impact assessment there, but even if there were a privacy impact assessment, you could imagine that the scope of a particular investigation either would be within that PIA or could go beyond what is contemplated by the PIA. There is no example or no instance that you've been provided, at least that you're aware of, where the use is obviously beyond the bounds of anyone's expectation of privacy.

Mr. Philippe Dufresne: There hasn't, but it highlights, again, another recommendation that I've made and that this committee endorsed in the ODIT study, which is the element of necessity and proportionality. That too should be in the law, because that's the point you're getting at. There may be a legitimate purpose. However, are you going too far in how you're achieving it?

Mr. Nathaniel Erskine-Smith: Yes, the scope of the search matters, depending upon the context and what you're after and the seriousness of any allegation—if it's relating to employee harassment, for example.

Those are all my questions, but I will say, Commissioner, that if you do have examples that you feel have gone beyond reasonableness, have gone beyond necessity and proportionality, I would appreciate it if you would refer back to the committee on that.

Mr. Philippe Dufresne: Thank you. It's noted.

The Chair: Is that it?

Okay. Thank you, Mr. Erskine-Smith. You did have a little more time left. I appreciate that.

That concludes our first round. We're going to reset the clock now and go back to six-minute rounds.

We are going to start with Mr. Barrett.

Mr. Barrett, go ahead, please.

Mr. Michael Barrett: Can you explain to us the distinction between data or information that is stored on a device and information or data that is only accessible via the device in Canadian law?

The relevance of my question or the precision that I'm looking for is with regard to the regular use of cloud-based storage. While the physical device might be the property of the Government of Canada or a government department, for an individual who has logged in to cloud-based storage of their information, the information isn't stored on the government's device but is accessible via that device through the individual's personal log-in credentials. What's the difference in law?

Mr. Philippe Dufresne: We would look at that as personal information about the individual being personal information relating to them. Whether it's on the device, on the cloud or in some other form, among other things, we look to see the following: Is this information protected appropriately? Who is gaining access to this? Who has control over this information? Is it legitimate for the government to seize that information? What are the boundaries?

We wouldn't draw too much of a distinction on that in terms of whether it's on the cloud or on the device. What we would really look at is the basis for obtaining it, the technology being used and the expectations of the individuals. Those would all be questions we would ask in that context.

Mr. Michael Barrett: There's no limit, then, to the reach of the government in using this technology in spying on Canadians. Microsoft—lots of folks use Microsoft to store their documents—Dropbox and Google are all cloud-based. People store family photos in there. They store personal correspondence in there. They store confidential and private medical information in there.

Would it ever be appropriate for the government to use the guise of saying, “Well, it's a government device, and you once logged into your cloud-based account using that device. Therefore, we now have unfettered access to that”? Is the only measure after the fact: what they looked at and, “Oh, well, we only took certain things”?

Once they've viewed the information, the privacy of the employee has been violated. That Canadian's privacy has been breached. Is it ever appropriate?

● (1210)

Mr. Philippe Dufresne: There's a principle of limiting collection, again linked to necessity and proportionality. If you're the employer and you're going to be looking at the data of the employee, it's all part of the transparency. Make sure the employee is aware that this is their work device. If they're using it for personal things, is there a mix? What are the expectations in terms of what the employer will have access to? Why does the employer need to have access to those things?

It's all about making sure the employer or any other organization doesn't get to collect and use more information than they need. That means looking at the purpose and looking at the context. I gave the example of truck drivers being filmed on their personal time. That wasn't necessary for safety on the roads.

Similar types of questions would be asked. The more you're going to go and get my personal information, the more you should have to justify why that is. Again, that's what privacy impact assessments do, and that's what necessity and proportionality would do. We live in a time where that technology, as you described, is more and more invasive. Sometimes there's a mix between the personal life and the work life, so that raises privacy implications.

Mr. Michael Barrett: Will the PIA be used to approve the software or technology that the government plans to use, or is there a process? In advance of collecting the information, ought there not be a requirement for any government department to have the technology, that specific software, pre-approved? On this distinction that it's just employees of the Government of Canada, that's a pretty big employer in this country. The employees, by and large, are Canadians, and that's not to be glossed over.

We seem to be playing catch-up so often on privacy issues with government and government departments. Would your recommendation be that the software be approved even prior to procurement?

Mr. Philippe Dufresne: I'll read you 4.2.2 of the “Policy on Privacy Protection” from the Treasury Board. It says:

> Notifying the Privacy Commissioner of any planned initiatives (legislation, regulations, policies, programs) that could relate to the Act or to any of its provisions, or that may have an impact on the privacy of Canadians. This notification is to take place at a sufficiently early stage to permit the Commissioner to review and discuss the issues involved.

It's that same point. Do it before, not after, so we can flag concerns.

The Chair: Thank you, Mr. Dufresne and Mr. Barrett.

Ms. Damoff, you have six minutes, please.

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

Thank you so much for being here today and shedding light on this serious issue.

First, I want to ask you this: Is this spyware?

Mr. Philippe Dufresne: This is not spyware. The difference is that spyware is covert and remote. You don't have the device, and you're doing it. This is a digital forensic tool, so it's a different type of tool.

Ms. Pam Damoff: Okay. It's been referred to by my Conservative colleagues a couple of times today as “spyware”, so I just wanted to clarify that.

I remember back in 1996, before the days of these kinds of phones, I was working at Midland Walwyn in real estate investment banking. I knew that IT was monitoring what was on my desktop. I was told that. This was my work desktop. It was to be used for work. That extended to even when I had my House of Commons iPhone. I know it's a work phone that is supposed to be used for work.

I have an Apple watch like my NDP colleague. It's on my personal phone.

Why would the government have access to personal health information unless someone has chosen to put their private information on a work phone when they know that phone is only supposed to be used for work? I'm a bit confused by that.

Mr. Philippe Dufresne: We talk about that in our "Privacy in the Workplace" document that we revised in May 2023. It's really talking about the monitoring and the transparency. To your point, if you as an employee are aware—here's what the employer can and can't do, here's what the tools of the employer can do if you use this tool—then you have that awareness as the user. You have that transparency.

There may be circumstances where it's absolutely warranted for the employer to have access to certain things. However, even if the information is there on the phone, why would the employer need to have access to that health information of yours? You put it there, perhaps rightly, perhaps wrongly, but does the employer need to have that?

How do we balance that—limiting the use, limiting the collection, and that transparency? We have to modernize and apply these rules to evolving technology. It was much easier before, because, as you say, with these devices so much of our lives are so much easier to mix up.

We were talking about the RCMP's use of ODIT before, and that was really done because the wiretaps weren't working anymore. People weren't using landlines. However, the landline didn't give you nearly as much information as the phone. That's an example of a different tool, but it also is of a greater magnitude.

● (1215)

Ms. Pam Damoff: I've had those questions for the RCMP before. I used to be on the public safety committee.

I am a bit confused about that, because I think, if I'm not mistaken, Apple has won court cases not to provide passwords to access smart phones. I've heard from police services and the RCMP that they're stymied in cases, because they can't access that information, where legitimately it could be organized crime.

From what I'm hearing today, it makes it sound like the RCMP actually have access. We're talking about employees—are we not? We're not talking about the organized criminal out there they would like to have access to. I think the lines get a little bit muddied here about what exactly we're talking about when it comes to our police services.

Mr. Philippe Dufresne: In the context of the RCMP, in this instance they're using those tools for their investigations generally. They're not investigating their employees. Three of the organizations are doing them for internal investigations.

Ms. Pam Damoff: They have to have the phone, though. They would have to bring me in and I would physically have to provide them with my phone. Is that right?

Mr. Philippe Dufresne: Right.

Ms. Pam Damoff: This isn't being done surreptitiously, where a Canadian is sitting in their home and the RCMP is surveilling their personal information.

Mr. Philippe Dufresne: That's right. It's not the same thing as spyware. It's done when you have the device, you're going on the device and you're retrieving information.

Again, in certain instances it may be perfectly legitimate for the RCMP or for an employer to have that information. The issue is that we need to make sure that it's done with privacy protection in mind. We need to make sure that there's transparency and that there are these guardrails. I don't want to suggest that the use of this is completely unacceptable and has to be stopped altogether. It's bringing this privacy lens to it so that we can have the benefit of the tool and at the same time protect our fundamental rights.

Ms. Pam Damoff: Have you found out what the departments were using this tool for? I mean, I've heard fraud, harassment.... Do you know of any other instances where this tool was used?

Mr. Philippe Dufresne: We do. We've obtained information. Some have used it for anti-spam legislation. Some have used it for cybercrime investigations or national security matters. Some have used it for income tax purposes or investigations. Some have used it for the Competition Act, environment, fisheries, conservation programs, transportation investigations—these types of things that fall under the authorities of the departments. Three of them were for internal investigations.

Ms. Pam Damoff: I have only 15 seconds left, so can you provide us in writing with any recommendations you have?

Mr. Philippe Dufresne: We can—certainly.

Ms. Pam Damoff: Thank you.

The Chair: Thank you, Ms. Damoff and Mr. Dufresne.

[*Translation*]

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

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

I would like to move a motion that was sent to the committee in both official languages.

> Considering that the *Privacy Act* hasn't been reviewed since 1983,
>
> Considering that the ETHI committee asked for a review in its previous reports,
>
> That the committee ask the Government of Canada to review the *Privacy Act*.

The Chair: Thank you, Mr. Villemure.

The motion is in order. That said, I see only one problem: The committee does not have the power to ask the government to do something; it can simply make a recommendation. I would suggest replacing the word "ask" with "recommend".

● (1220)

Mr. René Villemure: “Recommend” is fine, but it must be noted that we have already made this recommendation. We are simply reiterating it. So I do not see a problem with that.

The Chair: Okay. Thank you, Mr. Villemure.

Mr. Dufresne, could you please stay while we discuss the motion.

Does anyone wish to comment on Mr. Villemure's motion?

[*English*]

Ms. Khalid, I see your hand up. Go ahead, please.

Ms. Iqra Khalid: Thanks, Chair.

Some of colleagues are online, and I'm wondering if I can take a two-minute suspension to confer with them.

The Chair: I'm just confirming with the clerk that the motion has been sent to everyone's emails.

I will allow a quick two-minute suspension so that you can discuss it, if no one minds.

Thank you.

● (1220)

_____(Pause)_____

● (1220)

The Chair: We're back from our suspension. As I mentioned, the email has been sent on the proposed motion from Monsieur Villemure.

Go ahead, Ms. Damoff, on the motion.

Ms. Pam Damoff: Thank you, Chair.

As the committee knows, the government is currently reviewing the Privacy Act.

My question for the member is this: Why would we pass a motion on this as opposed to including it in the report? We just started the study today. I'm wondering if he could maybe let us know why this wouldn't just be a recommendation of the report we're going to do on this.

The Chair: Yes, I think that's a fair question. Mr. Villemure and I had a sidebar on the exact same issue, but I will let Mr. Villemure explain.

[*Translation*]

Mr. Villemure, please explain your position to Ms. Damoff and to the committee.

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

The committee has requested a review of the Privacy Act on numerous occasions. Treasury Board announced a review of the act in 2021. As part of that review, I believe every Canadian is being consulted individually, which is time-consuming. The committee has already made various recommendations. Mr. Dufresne is with us this morning and I believe he has told us a million times that a review is needed. So we have to emphasize the need to discuss this again because it seems that the recommendation has not been taken seriously.

It's like anything else: Repetition eventually becomes untenable. We have seen built-in tools. There have been other studies about privacy. Every time, a review of the act was recommended. All of this will ultimately lead to something.

I think the committee is in agreement since we have heard the same testimony. The commissioner who is present and his predecessor told us the same thing: There is cause for concern. AI will completely change the situation. Even if the tool changes and the 1983 act remains in effect, the rest of the world has changed.

After making the first recommendation in two reports, we have to support the motion in the public interest. I want to stress that again.

● (1225)

The Chair: Thank you, Mr. Villemure.

[*English*]

Ms. Damoff, go ahead.

Ms. Pam Damoff: Thank you for that, I do appreciate it. The government does take it seriously. That's why the review's going on, but I appreciate the honourable member's desire to get this out there and make the point, and also the knowledge he brings on this issue.

Thank you for that.

Do we need to amend the motion, though, Chair, based on what you said just before?

The Chair: I think Mr. Villemure has already indicated that.

[*Translation*]

That's right.

[*English*]

Ms. Pam Damoff: How does it read now?

The Chair: We're changing “ask” to “recommend” because, as I said earlier, the committee does not have the authority to ask the government. We can recommend to the government, and I think that's what Mr. Villemure's intention is here.

I see Mr. Erskine-Smith.

Go ahead, please, on the motion.

Mr. Nathaniel Erskine-Smith: I'm not opposed to the government's reviewing the act. I think I was part of the ethics committee when we recommended this in the first Parliament I was part of in 2015-19.

However, to Mr. Villemure, I'd ask this: Isn't this a bit of a moot point and a waste of time? Isn't the government just going to come back and say what they said in response to the last report we're reviewing? Wouldn't it be more effective to put it, consistent with the evidence of the commissioner, in a short report and hammer home that we've done this many times, cite those many times, and say that we're asking for it to be updated, not only reviewed? It seems like this is a weaker version of what we could potentially do.

The Chair: I appreciate that, Mr. Erskine-Smith.

If this motion is adopted, this can be a motion that goes into the minutes of this committee's report and then of course, as we deal with the draft report after all the witnesses are done, it can be prominent and prevalent in that report. In the meantime, this is what Mr. Villemure has proposed and what we're dealing with right now.

I appreciate your input on that, Mr. Erskine-Smith.

[*Translation*]

Do we have a consensus on Mr. Villemure's motion as amended?

Voices: Agreed.

(Motion as amended agreed to)

[*English*]

The Chair: Thank you again for your patience, Mr. Dufresne and Ms. Ives.

Monsieur Villemure, you have the floor for six minutes.

Go ahead, please.

[*Translation*]

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

Thank you, colleagues.

Commissioner, I would like you to talk to us about the impact of AI on privacy and whether this is something that should be considered in the case of the 13 departments and agencies that are being investigated currently.

Mr. Philippe Dufresne: AI is a key element that affects the privacy of Canadians and people around the world. This summer, my G7 counterparts and I issued a resolution at our annual meeting reiterating the importance of protecting privacy. We reiterated the importance of implementing current legislation and the need to modernize that legislation and consider the effects of AI from the outset.

In October, my provincial and territorial counterparts and I also issued a statement. On December 7, we held a symposium here in Ottawa with our counterparts from other countries, and issued a statement about AI based on Canada's privacy principles. We also stated our expectations, specifically regarding legal authority, appropriate objectives, necessity and proportionality, accountability and limits of use. We applied that lens to AI.

With regard to the tools under discussion today, I have not been told that this involves AI, but that is a possibility we must certainly bear in mind. With regard to employment, the resolution issued by the Global Privacy Assembly last fall referred specifically to the use of AI in employment matters, including staff management and recruitment.

I cannot go into any details, but right now we are looking into a complaint against OpenAI to determine whether the company is in violation of the act with ChatGPT. We are also considering what to recommend if it is in violation.

There are also all the issues relating to the data that is used to train AI. What is protected and what are the limits? The Organization for Economic Cooperation and Development conducted a study on AI with G7 ministers, and the three greatest risks identified were disinformation or misinformation, the effects on copyright, and the effects on privacy. So this is a very important issue.

Last week, the Office of the Privacy Commissioner of Canada announced its three strategic priorities. The first is optimizing and modernizing the office's structure to ensure we have the maximum impact. The second is ensuring that technology respects privacy and that people can utilize it but with guidelines. The third is protecting children's privacy, another extremely important element. In addition, the CEOs of social media companies appeared before the U.S. Congress this week to talk about their impact on children. These priorities are at the heart of our work.

● (1230)

Mr. René Villemure: Over and above your three priorities, would you say the Office of the Commissioner is currently equipped to assess the impact of AI on privacy?

Mr. Philippe Dufresne: We are well equipped to do so. We have a technology laboratory, but we have more work to do. It is an evolving situation and the organizations we regulate definitely have more resources than we do. We have to continue in this direction and we will focus on it.

Mr. René Villemure: You mentioned ChatGPT, which is generative AI. Have you seen a different effect on privacy since the emergence of generative AI or, rather, has it simply accelerated the current effect?

Mr. Philippe Dufresne: We are seeing that it is being used more and more. We can see the potential impact of false information and of using someone's image to make it look like they are doing something. Generative AI poses tremendous risks to privacy and dignity, so the challenges are certainly greater.

Mr. René Villemure: The image of an American comedian who died in 2008 was used recently in a new show. The video isn't perfect, but the voice, tone and comments are the same. Current events are discussed.

Would you say this kind of thing is a violation of privacy?

Mr. Philippe Dufresne: I would say that could indeed be a violation since personal data is being used for purposes that are not acceptable or accepted. It has an impact on dignity and raises all sorts of risks and issues. So it is something that has to be looked at.

People need to know what can be done with their personal data. So protecting that data is even more important. If someone has access to my voice and the way I talk, they can use AI to harm me or to harm others.

Mr. René Villemure: According to the World Economic Forum, disinformation, or misinformation, and privacy are the main concerns.

Would it be possible to obtain the public statements that Canada and your G7 counterparts made last year?

Mr. Philippe Dufresne: Certainly. Those statements are public and are posted on our website. I can have them sent to the committee, including those pertaining to employment and protecting children's privacy.

Mr. René Villemure: Thank you very much.

I know my colleague Ms. Khalid is very concerned about protecting children's privacy.

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

[*English*]

Mr. Green, you have six minutes.

Go ahead, please.

Mr. Matthew Green: Thank you.

I appreciate being able to go back to the point about the human context of surveillance. We certainly delved into that when we talked about AI and its use for surveillance that was on-device in the audit response. We covered—I think, compellingly—the ways in which bias is baked in.

What I'm struck by in this way is surveillance that was more akin to CCTV. You know that in places like the U.K. and the United States, where there's an expansive use of CCTVs, they're found to be really susceptible to abuse, just based on human nature. The American Civil Liberties Union identified four ways in which CCTV is susceptible to abuse, so for the purpose of this round, I want you to just consider that context.

The first is criminal abuse. In instances like this, obviously if the federal government is doing it, the legality could suggest criminality if it's warrantless and outside the scope of their work. The second is clandestine, if we're talking about our RCMP, our national defence or perhaps more specifically our national security establishment and the way it does online surveillance. I'm not suggesting they're involved in that, but that is a possibility. The third is institutional abuse, the overreach, the top-down approach and the way in which government institutes surveillance on the public is a significant risk. CCTV was found to be not only ineffective but also, it was argued, an institutional abuse.

I think what I'm most concerned about with the sensitive nature of the information is the abuse for personal purposes, which is why I was trying to drill down on exactly who. I think, for anybody who's not aware of IT, we have an idea of who's on the IT side.

Would you agree that the intentions or the possibilities, the susceptibilities, for abuse at the level of CCTV or the analog level ought also to be considered at the deeply digital level, particularly as it relates to AI and the technologies and the full and complete access that it has to people's personal information and data? Is that a fair assumption?

● (1235)

Mr. Philippe Dufresne: I agree.

I think the more powerful the technology is, the broader the scope, the more you have to be careful and the more privacy protections and considerations you need. That's what proportionality is. You have this more intrusive tool, so you need to have a more rigorous protection mechanism.

I agree with you. The human element is important. We're talking about privacy as a principle. It's a fundamental right, absolutely, but it means that, at the human level, we're all less free if we lose our privacy, if we're living a life where we feel that we're constantly under the microscope and that people can see what we're doing, where we're doing it, what we're buying....

I point to one of the earliest articles on privacy called “The Right to Privacy”. They gave the example in the 1800s of someone who was collecting rocks and said that privacy means you're allowed to do that and not everyone in the village gets to know which rocks you're buying. That's your information.

Today, obviously, we can see that it's even more powerful. This is part of our freedom and our individuality, so we need to make sure that reflex.... It's not to say that you can't use technology—you can—but we have to do this bearing in mind privacy.

Mr. Matthew Green: I want to get back specifically to the PIAs. Do you have any way of knowing who has access to the information in the technology that you're reviewing? That's the first part.

Second, are there any current legislative or reporting mechanisms that would identify how often somebody's doing it? For instance, knowing that I have access to this type of, what I'll call, “digital voyeurism” is one thing, but not knowing how many times I'm using it is something completely different. In the case of CCTV, the voyeurism became a real thing when it became.... For police departments, there was evidence that they were using it to stalk women, to get information on their spouses or their ex-wives, and so on and so forth.

Do you currently have any mechanisms in place that would provide safeguards against this technology, which you may have approved in departments but for which you don't actually have oversight?

Mr. Philippe Dufresne: There is a range of tools. There are the private information banks of the government indicating what we have as information, why and what the purposes are. It's a type of proactive disclosure. Privacy impact assessments would be another way of proactively informing us of that use. Then again, it's making sure that not too many people have access to the information—

Mr. Matthew Green: But clearly you don't know that—do you?

Mr. Philippe Dufresne: We don't know that until we are provided with that information.

Mr. Matthew Green: The other issue that I have with the reporting is.... It seems to be the case with government...and again, I'll chalk it up to human nature and not necessarily make it a partisan jab. I'll just state that it is often the case that people only hold accountability when they're caught. The issue that I have right now is that we've only identified about a dozen organizations.

If you check your email accounts, you'll notice that I put a motion together. I'll speak to the motion while you guys look at your accounts because the inventory of federal organizations and interests identifies 137 departments or organizations under the federal public service. We're talking about 23 ministerial line departments, three service agencies, 17 departmental corporations, 15 departmental agencies and 12 special operating agencies. It's pretty far-reaching. The issue that I have is that we're only currently talking about 12. We don't know in this committee exactly who's using this and what the scope and scale of the use of this is.

What I'd like to do is move a motion. I move:

> That, in relation to the study on the use of tools capable of extracting personal data from telephones and computers by government institutions, the committee write to each federal department and agency not already named in the study and request that they confirm whether or not they have procured or have access to software used for extracting information off of electronic devices; and request that the response be sent to the committee no later than 10 business days after receipt.

● (1240)

The Chair: Thank you, Mr. Green.

The motion, as Mr. Green stated, had been sent to everyone's email prior to his moving that motion. The motion has been moved. I'm going to accept it because it is in relation to what we're studying today.

Is there any discussion on Mr. Green's motion? I don't see any.

(Motion agreed to)

The Chair: Thank you, Mr. Green. That concludes your time. The motion has been adopted.

We're going to go with five minutes, five minutes, two and a half minutes and two and a half minutes to conclude.

I know that everybody is aware that Mr. Barrett will be moving a motion at the end of this meeting. We should dispose of that fairly quickly.

We're going to commence our five-minute round with Mr. Kurek.

Go ahead, Mr. Kurek.

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

I think that the passing of that motion highlights a concern around the unknowns that exist. When I saw that Environment and Climate Change....

I represent an area with lots of farmers. There have been concerns highlighted to me by farmers who get correspondence from different levels of government. They don't know what certain demands are, what they mean or what's included in that. They're asked to agree to things that they don't necessarily have all the details about.

The fact that there are unanswered questions highlights how important it is to really get to the bottom of this. If that is impacting the privacy rights of Canadians, certainly we need to be very clear on that.

There's also the fact that Environment and Climate Change Canada recently had a job posting where they were looking for climate enforcement officers. What does that look like? Farmers in my constituency are asking what that looks like. I certainly would ask those questions.

Commissioner, you've outlined some of the concerns. I would, if I could, ask you to provide some specific examples of what needs to be changed in order for you to not only have the tools but to ensure that the legislative framework is in place so that the questions that we have asked—and all parties have asked—can in fact be answered. Those questions are not currently able to be answered because of gaps or because of regulatory frameworks that don't go far enough in Canada.

Could you outline some of those things?

Mr. Philippe Dufresne: Sure. Thank you.

I would recommend that a PIA be required when new, powerful tools can have an impact on the privacy of Canadians. Perhaps moving away from the notion of a program itself, if there is a new tool that changes the context, then consider a privacy impact assessment.

I would recommend making it clear that my office has to be consulted and advised before the deployment of new technology and before changes to new programs—not after the fact. In fact, it would be not just on the day of, but with sufficient time so that we can provide meaningful input.

I would recommend that the Privacy Act be modernized to include necessity and proportionality, which is this element and this discipline of saying, the goal may be important, but are we limiting the information that we're gathering to the minimum required?

Those would be highlights.

I echo the recommendation of the committee in terms of privacy by design. Also, of course, order-making powers for my office is something that is important and should be included in new law as well.

● (1245)

Mr. Damien Kurek: Yes. It's too bad that we need to even consider order-making power when I would hope that the attitude would be to presume privacy and to presume that privacy matters for Canadians. Obviously, over the four years or so that I've served on this committee, that is not the case.

Whether it's order-making power or when there is non-compliance, I'm curious where penalties, proportionality.... What would you recommend as the solution to ensure that ultimately, at the end of the day, this is not just a recommendation or a Treasury Board mandate that gets ignored, with nothing happening to those who wilfully ignore what could be the privacy rights of Canadians?

Mr. Philippe Dufresne: In the context of the private sector, I've clearly recommended order-making powers and fines in appropriate cases—and not because I want to issue fines. I want them to be a possibility because it focuses the mind of the decision-maker.

In government, I would hope that's not required for government departments, but it always—

Mr. Damien Kurek: Do you have a number? I'm just curious. You mentioned fines. Is it an administrative penalty? What is the thought?

Mr. Philippe Dufresne: In a private sector context, they're talking about a percentage. I think it's 10% of takeaway in a year for an organization, or $10 million or $15 million—I forget the specific details—but you have that range.

For government departments, it could something different, although you have also Crown corporations. We've issued a decision on Canada Post in our annual report. We're waiting for Canada Post to comply with that. They have not—yet.

These types of tools are helpful.

The Chair: Thank you, Mr. Kurek.

Thank you, Mr. Dufresne.

Mr. Erskine-Smith, I have you next for five minutes. As you started last time, you said “hey” to the analysts. I know that you spent three years on this committee and, on behalf of the analysts, I'm going to say “hey” back.

Voices: Oh, oh!

The Chair: They wanted me to say “hey” back. I know they weren't going to do it, but I did it.

Go ahead for five.

Mr. Nathaniel Erskine-Smith: Thanks, John.

Thanks, Alexandra and Maxime-Olivier.

Commissioner, my colleague Matthew Green drew a parallel to CCTV. There is no question, then, of documented abuses of CCTV. This is of course a different technology, and different technologies have different challenges.

It strikes me that in this particular instance, with this particular technology, there are two considerations and potential concerns for you to look at. One is whether the search of a device is warranted and justified—that's number one—and then whether the scope of the search of that device is reasonable, necessary and proportionate.

Does that sound right?

Mr. Philippe Dufresne: Yes. I agree with that.

Mr. Nathaniel Erskine-Smith: Okay. That being the case, of the departments that have deployed this technology.... You said that one of the 13 hasn't, but of the departments and agencies that have, how many times has it been used?

Mr. Philippe Dufresne: How many times has it been used? I might need to get that detailed information for you. I think some of them have said just on a handful of occasions, and others I don't think have specified. I don't have these specific details. I can see if we can provide that subsequently.

Mr. Nathaniel Erskine-Smith: Okay.

Subsequent to that, how many times has it been used absent judicial authorization? In a number of the instances that you're suggesting, whether it's fisheries or the RCMP, it sounds to me like it's not actually about employees. It's pursuant to investigations. It's potentially the same with the CRA.

It strikes me that where it's an investigatory body that has due process wrapped around their other investigatory mechanisms, probably this flows within that other due process. You'll do your work on the privacy end, but I'd be a little less concerned if there is sufficient due process already baked into the consideration, whereas if it's used for other reasons—non-investigatory, pursuant to an act, pursuant to existing due process—we might have concerns. Does that sound right?

● (1250)

Mr. Philippe Dufresne: Yes, and that's one of the things that I would look at also in the context of a privacy impact assessment: getting those details. What's the context? What are the safeguards?

Mr. Nathaniel Erskine-Smith: Right, and it seems to me that, in the course of your investigation here and in your questions, you ought to be reaching out.... It would be better—and I appreciate Mr. Green's motion—and you're better placed, actually, to reach out to these other organizations and ask those very same questions and then revert back to us. We could oversee your work because we have powers that you don't, but you have the time and inclination to do the detailed work of asking the questions.

In the course of asking those questions, it would be good to know how many times it's been used absent judicial or other authorization pursuant to existing due processes for investigations and—this is getting to my previous inquiry—two, whether there are instances where they're searching government devices pursuant to an internal investigation like harassment. That's another category where I think it makes a lot of sense to me that it would be used.

Now you get to the subsequent concerns around scope of search, and you will want to inquire as to scope of search. If there are concerns about scope of search, I would again ask you to revert back to us. It would be good to know if this is being used in other instances, any concerning instances, that don't involve investigations that on the face of it seem reasonable.

My last question.... You'll get back to us on a number of uses. On scope of search, as you look to privacy impact assessments and working with these agencies on privacy impact assessments, it would probably be good.... Let's take the concern that Mr. Barrett raised about the difference between a government device and the cloud—fair point. Now, your point back—rightly—is that one has a reasonable expectation in one's privacy, and one has different expectations of privacy in different material. One protects that reasonable expectation of privacy with the bounds of necessity and proportionality.

I would be very interested to know if departments, in the course of their investigations, have gone beyond the bounds of necessity and proportionality. Are they searching the cloud unnecessarily in the course of harassment investigations? Are they searching in health info? I mean, it's a theoretical concern of this committee. Did it actually happen?

If, based upon your investigation, you could come back to this committee with real concerns identified, it would be appreciated.

Mr. Philippe Dufresne: Thank you.

I have taken note of all of those elements, and we will follow up and report back to you.

Mr. Nathaniel Erskine-Smith: Thank you.

The Chair: Thank you, Mr. Dufresne.

Thank you, Mr. Erskine-Smith.

[*Translation*]

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

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

Commissioner, we have heard a lot of recommendations today, which we will of course consider. Looking ahead, though, what is on the horizon? What are we not seeing? What should the committee be considering to better anticipate things? New things have been coming at us quite quickly in recent years and I think we are still somewhat behind, if not several steps behind.

What would you recommend for the committee to get ahead a bit?

Mr. Philippe Dufresne: In the strategic statement that we published last week and that I will forward to the committee, we talked about three priorities.

The first is modernizing the office and maximizing its impact through new legislation. At the very least, if there is no new legislation, we will have to examine how to protect privacy as much as possible.

The second is technology. We have to get ahead of technology or at least keep up with the pace of developments. That is a big challenge because we can see that people are increasingly adopting it. People like technology, use it and see its benefits. So we have to make sure that their privacy is considered and protected.

The third is protecting children's privacy. This is a very challenging area. It impacts their mental health, their reputation and their data. So there is work to be done in this regard and we will be focusing on these areas.

Internationally, there is also the issue of protecting data that flows across borders.

In short, by focusing on technology and trying to anticipate its trends and uses, and by focusing on children and their privacy, we will be focusing on the future. That is why we will be focusing on these areas. We are also open to recommendations the committee might have for us on other matters.

For my part, I take a broad view: We want to make the most of innovation and technology for the many advantages they offer in multiple fields. Mr. Green talked about the use of technology in health care, and it can also be helpful in sports and music. It can be beneficial and we must not refuse everything. Yet I do not want Canadians to have to make a choice between the advantages of technology and maintaining their privacy. They should not have to make that choice and the burden should not be entirely on individuals. I want Canadians to feel and know that institutions are there to protect them and advise them.

● (1255)

The Chair: Mr. Villemure, if I understand correctly, Mr. Green has given you his speaking time, so you have another two and a half minutes.

Mr. René Villemure: That's great, thank you, Mr. Chair.

Commissioner, to keep abreast of the latest trends, do you attend the Consumer Electronics Show in Las Vegas, for instance? How do you go about that?

Mr. Philippe Dufresne: We are very active in certain communities in Canada and internationally to keep up with developments. Some privacy communities also involve the industry, which presents its products. At our office, we have a technology laboratory that keeps abreast of the latest developments in technology.

That is in fact the office's second priority. We do not want to tell people to stay away from technology because it is dangerous and impacts their privacy. We want to use it responsibly ourselves so we can then tell people how to use it while protecting their privacy. That way, people will not have any reason not to use it because we all know it is possible. We do not just say that it should be used responsibly; we do so ourselves.

Mr. René Villemure: Regarding children's privacy, of course we want to prevent potential abuse, harm and injury. For a young person today whose first photograph was taken in their mother's womb, privacy is a vague concept. Entertainment often comes before protecting privacy. Most young people typically say the same thing, that they have nothing to hide, something you no doubt also hear. Yet we know that is not the case.

What will it take to educate the next generation for them to properly understand the importance and value of privacy?

Mr. Philippe Dufresne: You're right. Young people are very familiar with technology, probably better than older people in some cases. We need to strengthen the awareness of privacy though, among young people and their parents alike. I am thinking of parents who overshare, for instance, since parents often post information on social media. The children suffer the consequences of that for a long time. The legal system therefore needs to be prepared to protect their privacy and we have to have those conversations.

I would like to see schools institute mandatory instruction to make young people aware of protecting their privacy. Since education is clearly under provincial jurisdiction, we work closely with our counterparts. We issued a joint statement on protecting the privacy of young people that calls upon industry, governments and educators.

Just as we teach children about safety and tell them not to get into a car with a stranger for instance, we should warn them that, even if there is something very interesting, they need to think about the consequences.

Mr. René Villemure: Last week, a constituent was telling me that her nine-year-old daughter does gymnastics and went on YouTube to watch gymnastics videos. One thing led to another and she happened upon pornographic images of young gymnasts. To attract her, her privacy had to be compromised. I was shocked that this little girl who was watching videos of an Olympic gymnast ended up somewhere else on the Internet. So action is needed to protect children's privacy and to raise their awareness.

Thank you very much.

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

That brings today's meeting to a close.

Mr. Dufresne, on behalf of Canadians and the committee, I want to thank you for your testimony today on this very important matter.

Thank you also to Ms. Ives.

[*English*]

We have a couple of items to deal with.

First, I'll go to Mr. Barrett.

Mr. Barrett, you have an oral motion that you'd like to put before the committee. I understand that you've spoken to committee members, and they all are in agreement with it. If you would put the motion on the floor, then we could have some discussion, if need be, on it.

Go ahead, sir.

Mr. Michael Barrett: Would you like me to put the motion on the floor and then speak to it very briefly, Mr. Chair?

The Chair: Yes, please.

Mr. Michael Barrett: The motion that's been circulated is as follows. I move:

> That the committee send a letter of condolences to the family of former Ethics Commissioner Mary Dawson that recognizes her lifetime of public service, and that the committee report to the House an expression of its condolences on her passing.

The Chair: Okay.

The motion has been moved, and I'm going to rule it in order.

Go ahead, Mr. Barrett, please.

Mr. Michael Barrett: Mary Dawson passed on December 24, 2023. I want to share a couple of notable points about her and why this is so important. I appreciate colleagues' agreement for this to be before committee and to report it to the House.

She wasn't just the Ethics Commissioner. She was pretty remarkable. Her fingerprints are all over very important parts of our history, including her having drafted the Access to Information Act, the Privacy Act, the Canada Health Act, the Official Languages Act, the Competition Act, the Customs Act and the Young Offenders Act.

She was made a member of the Queen's Counsel in 1978 and became associate chief legislative counsel in the early 1980s. Aside from being the associate deputy minister of justice for nearly two decades, she was particularly proud of her constitutional work, including being the final drafter for the patriation package on the Constitution Act, 1982, and the Charter of Rights and Freedoms.

That is a very brief, incomplete and not fulsome summary of her impressive service as a public servant to our country and her work as commissioner in calling balls and strikes. I think the mark of a good Ethics Commissioner is one who makes members of all parties equally uncomfortable, and she did that well.

Canada was well served by her contributions, and I appreciate colleagues' consideration of the motion.

● (1300)

The Chair: I want to thank you for moving that motion, Mr. Barrett, and for those kind words on Ms. Dawson.

I never had an opportunity to deal with her directly, but certainly when you take the chair you're aware of the invaluable contributions she made, and not only as the Ethics Commissioner but, as you've cited, just what a phenomenal experience and a life of public service that she gave to this country.

Thank you for this motion.

Ms. Damoff, go ahead, please, on the motion.

Ms. Pam Damoff: Thank you, Chair.

Just very briefly, I want to thank my colleague for bringing this motion forward—we of course are happy to support it—but also for the quite eloquent description of Ms. Dawson.

I also didn't have the opportunity to work with her or know her, but I think you've done a really good job of describing her for Canadians, and I just want to thank you for bringing this forward. I pass on condolences from our side as well.

The Chair: Thank you, Ms. Damoff.

She is legend for sure.

Is there any other discussion? I assume we have consensus on the motion—

Mr. Matthew Green: There is unanimous consent—not just consent.

(Motion agreed to)

The Chair: Thank you for bringing that forward, Mr. Barrett.

[*Translation*]

We have to adopt one last motion. It pertains to the budget for our current study on the federal government's use of technological tools capable of extracting personal data from mobile devices and computers.

Mr. Villemure, if the committee wishes to adopt the budget, the amount is $16,500. That includes the expenses for the witnesses, video conferencing, the work report and other expenses.

Is it the pleasure of the committee to adopt this motion?

Voices: Agreed.

(Motion agreed to)

[*English*]

The Chair: Ms. Khalid, do you have one more quick item?

Ms. Iqra Khalid: I'm sorry. I have just a very quick question. I'm wondering about the timelines for the draft report on the social media study.

The Chair: Perhaps I can go to the analysts to provide that, and that did remind me about another issue that I have to bring up.

Ms. Alexandra Savoie (Committee Researcher): The report has been drafted. It is in the process of being translated. We should be able to distribute it in mid-February. I think the actual formal date that we have so far is the 19th. If we can provide it earlier, we will, but it should be the 19th at the latest, which is in the break week, so you'll have a week to review it.

The Chair: Okay.

I have just one more item. We adopted a motion the other day to send a letter to the procedure and House affairs committee, plus the Board of Internal Economy. The letter has been drafted. It's in translation. We should be able to share that with the committee perhaps later today. The request was to review and perhaps edit it. It's a very short letter, and not substantive at all, based on what the committee decided the other day.

I'm not seeing any other business. Have a great afternoon and a great weekend.

Thanks to our clerk, our analysts and our technicians for today's meeting.

The meeting is adjourned.