HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

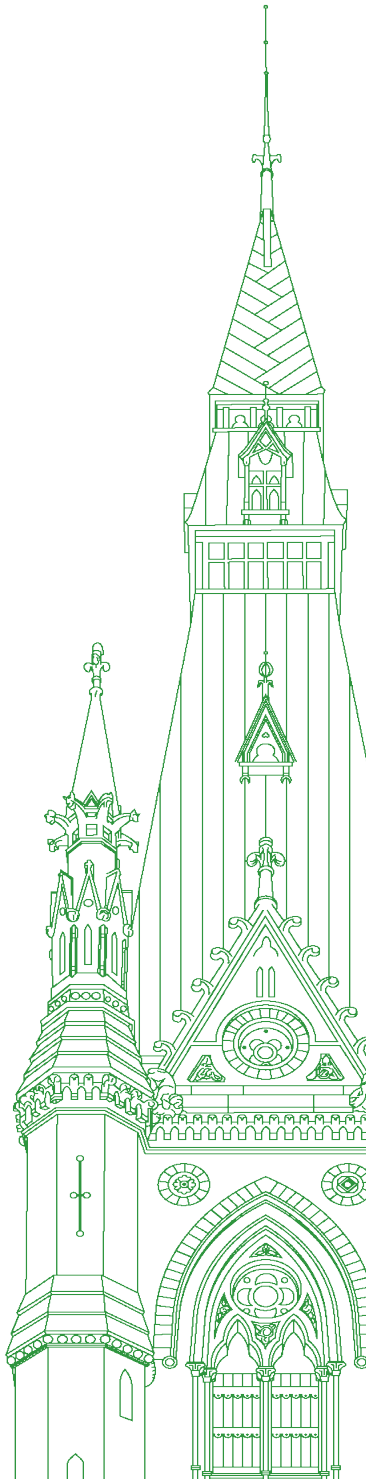
44th PARLIAMENT, 1st SESSION

Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 104

Thursday, February 15, 2024



Chair: Mr. John Brassard

Standing Committee on Access to Information, Privacy and Ethics

Thursday, February 15, 2024

● (1105)

[*English*]

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

I'm going to call the meeting to order.

[*Translation*]

Welcome to meeting number 104 of the House of Commons Standing Committee on Access to Information, Privacy and Ethics.

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

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

[*English*]

I just want to remind everyone again, as I always do, to make sure to keep the earpieces away from the microphones so that we don't harm our interpreters or Mr. Light.

I'd now like to welcome our first witness for this hour. As an individual, we have Mr. Evan Light, an associate professor.

Mr. Light, I want to welcome you to the committee. You have five minutes to address the committee.

Go ahead, please.

[*Translation*]

Mr. Evan Light (Associate Professor, As an Individual): Good morning, ladies and gentlemen.

My name is Evan Light, and I am an associate professor at York University's Glendon College.

[*English*]

I am an associate professor of communications.

I will give my opening remarks in English, but I welcome comments or questions in French, as well.

I am, as one of you mentioned on Tuesday, the source of the documents from which Radio-Canada has been doing the reporting since November 2023 on the use of tools capable of extracting personal data from mobile devices and computers.

The speed with which you've taken up the challenge of investigating the widespread use of mobile forensic devices throughout the federal government is, for me, quite impressive and demonstrates a deep respect for the fundamental human right to privacy. Privacy is not an abstract thing. It is a fundamental human right that is tied to other human rights. In Canada, it's been a human right since 1977. We're talking about something that's quite fundamental.

For me, that means it's a right that should not be violated unless we have a very good, well-documented reason to do so. I think the testimony that's been given to you by agencies so far hasn't necessarily shown that their use is what we could call “necessary and proportionate”, which is a term that has come up at various times during your recent meetings.

From 1977 forward, successive governments have failed to protect our fundamental right to privacy. This committee, at this moment, has a really great opportunity—not just an opportunity but an obligation—to step up and examine how government protects the fundamental right to privacy.

I've forwarded numerous documents to the committee. Some have been translated and some have not, so you don't have everything I'll be talking to you about today. I want to talk about these issues and get into some of the testimony from the agencies you've spoken with so far.

I first encountered these devices in 2020 when doing research for a course. A group in the United States documented their use throughout over 2,000 police forces in the United States. There's been further documentation by the Carnegie Endowment in the United States, documenting the use of these tools by various regimes throughout the world and how they're tightly integrated with spyware.

As a quick note on terminology, I don't see MFDs—mobile forensic devices—as being spyware. It's come up numerous times at this committee. However, they have essentially the same capabilities. They're sold by the same suppliers and they're used by the same entities. I don't think we need to get hung up on terminology. I think it's important that they are equally invasive and equally unregulated in their use—if not more widespread and more unregulated in their use.

My concern is not that these devices exist, but that their use is completely unregulated. Various agencies that have testified to you have said that they don't really know how they use them. They don't keep numbers. CBSA said they use them all the time, but they can't tell us how many times they use them. Shared Services Canada testified on Tuesday that they don't have any actual policies or procedures on how they use them. Scott Jones decides, as an individual, when their use is warranted.

As noted by witnesses to this committee, the devices are relevant. They've been renewed many times. I believe Mr. Mainville, from the Competition Bureau, mentioned on Tuesday that they've been using these devices since 1996, which was an amazing revelation to me. It shows that these things have been used regularly by government for decades. They have been and continue to be unregulated and without any oversight.

Throughout the committee meetings related to this study, members of the committee and witnesses have used the phrase “necessary and proportionate”, or portions of it. I think this phrase is really key to understanding the use of mobile forensic devices or any sort of surveillance technology by government. It's actually tied to a document that came out in 2014, which was developed by 16 civil society organizations around the world. It's been endorsed by about 600 organizations and around 300,000 individuals. It's called “Necessary and Proportionate: International Principles on the Application of Human Rights Law to Communications Surveillance”.

There are legal frameworks to work on. There are standards for understanding how to do surveillance while respecting human rights, which is something that I think Canada can learn from and maybe should.

I'll be quick. I'm almost at my five minutes. I'll finish with a quick note on some of the recent testimony.

Shared Services Canada and various other organizations have said they only use mobile forensic devices in isolated labs, which gives the impression that they're really cut off from the world. Based on the capabilities of the devices they own, this is patently false. In the contracts that I forwarded to this committee, various entities, including CBSA, CRA, ECCC, the RCMP and TSB all have what's called UFED Cloud, which is a software package from Cellebrite that essentially lets someone access any cloud applications that are on somebody's phone. It's advertised as a way to get around warrants.

In addition, as my last comment, various agencies have ruggedized versions of these devices. “Ruggedized” means they're able to go into the field and be dropped and thrown around. They would not be buying ruggedized devices if they were to be used only in isolated clinical labs.

I welcome any questions.

● (1110)

The Chair: Thank you, Mr. Light. I appreciate it. You had a little extra time there. That's okay for one witness. I don't mind giving a little extra time to a single witness.

Regarding the documents that Mr. Light referred to, there are literally thousands of them, and some of them are quite large. It would be quite the task to translate those documents, as you can imagine, but there are some documents that are being distributed to the committee based on what Mr. Light has provided us, and they are being translated.

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

Go ahead, sir, for six minutes.

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

Thank you, Mr. Light, for coming here and for the information and the workup that has led to this investigation.

I would just note—I guess this is a request because it's tough sometimes to get to the meat of the matter within the time frame of questions—that you did mention that there are some recommendations on how a government can ensure that rights are respected while investigations take place. I would ask if you could, with your expertise, send to the committee specific recommendations—generally, a recommendation could be a couple of sentences—and if you could distill that to a point where the committee could say, “Okay, here's something that we could recommend to the government.”

I would also just note, for your information, Mr. Light, that I've filed what's called an Order Paper question asking for some more details on this over the extent of the entire government. I know that 13 departments were highlighted. Shared Services Canada indicated that there may be more than 13, so I have asked this question, and I am hopeful that the government will be forthcoming with that information. I think it has 45 days to reply to that, so that's probably in about a month and a half.

You talked about the right to privacy and that it's been acknowledged as a human right in Canada since the 1970s. One thing that I've found very interesting and that has led to a host of concerns is the differentiation that you have of these very powerful forensic tools for use for administrative purposes within the context of a department to look at an employee's device in administrative investigations or something to that effect versus a court order for investigative purposes for someone who is not an employee of the department and didn't sign a terms and conditions contract but rather is the subject of an investigation or a periphery witness to an investigation.

Could I ask you to expand a bit on what the difference is and how one reconciles the difference between the use of these very powerful tools for administrative purposes within, say, a department or agency versus for investigations where they would be used on Canadians, whether with judicial authorization or the various other forms for which we've been told they could be used?

Mr. Evan Light: Regarding their use internally, I think that most of the representatives of agencies who have testified so far say, “We use them on our employees, and we get their consent.” It's difficult if not impossible for employees to give informed consent in these situations, because there's an imbalance of power, and there's an imbalance of knowledge. We've seen in sessions of the committee just how difficult it is to explain what these devices are capable of. Consider this: If you are a junior employee and your manager says, “We're going to use this device on your cellphone”, you have no real alternative other than to say yes. I think that use internally is quite fraught and imbalanced.

In terms of its use with warrants, I think there needs to be a step before you get to a warrant. If we are talking about “necessary and proportionate”, there are questions that we should ask. Is this technology valid to be used to begin with? This is where privacy impact assessments come in, which I personally think are useless to a degree.

They basically account for self-regulation right now. There's no process that agencies or ministries are obliged to go through that would forbid them from using any technology. We saw in Scott Jones' testimony on Tuesday that he will buy this for anybody in government who wants it. There's no standard, which is mind-blowing.

● (1115)

Mr. Damien Kurek: It's interesting that you bring that up. I've been very forthright in my advice—I reference it as unsolicited advice—to pick up the phone and call the Privacy Commissioner. We have an independent officer of Parliament, and any and all departments and agencies are a function of Parliament. I think that often gets forgotten.

Specifically with privacy impact assessments, if departments, agencies and the government in general were more forthcoming, doing things like privacy impact assessments and doing the outreach to the Privacy Commissioner prior to the use of these tools, do you think that would go a long way in helping ensure that the trust Canadians expect they should be able to have with government could be restored?

Mr. Evan Light: Personally, I don't think it would be enough.

The Office of the Privacy Commissioner should be properly resourced and empowered with judicial authority and with proper financial resources to be a proactive regulator. In the whole process of procurement, the Privacy Commissioner should be the one to decide whether or not technology should be used and in what use cases. I think that agencies themselves are in a conflict of interest, really, when it comes to making their own decisions around whether things should be used or not. There should be an objective arbiter, which would be the OPC.

Mr. Damien Kurek: Okay.

You're suggesting going beyond the privacy impact assessment and ensuring that there are more steps and more tools than the office has.

Mr. Evan Light: Absolutely. I think the privacy impact assessment is a useful tool for getting individuals and agencies to think about these ideas. I don't think it's a useful regulatory tool.

Mr. Damien Kurek: If you have those specific recommendations, please feel free to send them to the committee. Often it's a sentence or two that articulates exactly what you've suggested, and with your expertise and background as well, you are also welcome to send supporting documents. I know that there is a ton of other information, but please feel empowered that you are welcome to send that to the committee after your testimony here today.

The Chair: Thank you, Mr. Kurek.

Mr. Light, generally what we try to do at committee is set a deadline on when that information can be provided. I'm going to set that deadline for a week from today at five o'clock. The clerk will follow up with you and remind you of what Mr. Kurek's request was.

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

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

Thank you, Mr. Light, for being here today.

You were quoted in the CBC story as saying that you were troubled—deeply worried, I guess—by the information with which I presume you were presented by the reporter about the PIAs not being done in the 13 departments. You've heard, I imagine, the testimony from the different departments.

You don't in any way deny or disagree with their assessment that they're not using spyware or malware and seeking to spy on Canadians at large. Is that correct?

Mr. Evan Light: I have no evidence that would point one way or the other. I haven't done that research. I've done some.

Procurement is difficult to do research on. We work on contracts that are out there on the public record. I think that a lot of spyware companies sell their wares through third parties, so it's actually difficult research to do within government.

However, in the data that I've had, I haven't seen anything one way or another, so I cannot—

Mr. Anthony Housefather: No, but they have testified that they don't use it.

You have nothing whatsoever to contradict that testimony. Is that correct?

Mr. Evan Light: No, I don't.

Mr. Anthony Housefather: Okay. So, you have no basis to state the opposite. You just don't know. You're saying that you can't be sure that their testimony was truthful.

Mr. Evan Light: Exactly.

Mr. Anthony Housefather: Okay.

With respect to data extraction technology, you have to have the device in your possession. Do you agree with that? That's not spyware or malware.

● (1120)

Mr. Evan Light: You need to have the device initially. There are hardware components to mobile forensic devices that enable creating an image from a phone. Imagine that you're pulled over at the border and that you're asked for your phone. It can take maybe five minutes to make a copy of somebody's phone. Then you have an image, just like a CD image, that can be put on a USB drive and that can be shared between agencies. Data becomes a portable thing.

Mr. Anthony Housefather: Now you're saying that people are acting completing outside of the law, the limit of a warrant and the limit of their authority to do that.

You've had no testimony that has ever shown that any of that has happened. Is that correct?

Mr. Evan Light: That's correct.

Mr. Anthony Housefather: You have no basis to say that, other than your supposition that this is hypothetically possible.

Mr. Evan Light: That's correct.

As well, I'm going on the basis of just the capabilities of these technologies and what they are advertised for. For instance, if you look into the Cellebrite marketing materials, you will see that they advertise their cloud capabilities as ways to work around warrants. In the past, you would need to get a warrant to use anybody's cloud account, to access their banking through their phone, to access their Google Maps or GPS history, etc. With regard to the cloud functionality that I mentioned these five agencies have, they advertise it as a way to work around warrants. You no longer need a warrant. You just need a phone or an image of the phone.

Mr. Anthony Housefather: Again, I understand hypothetically what can be done with the technology. All I am substantiating is that we've had multiple people here who have testified, and none of them have said any of these things. As you know, when you're at a committee, whether you're sworn in or not, you are beholden to tell the truth under penalty of perjury or penalty of contempt of Parliament.

Nobody has testified to this. In fact, I'm just going to read what the CBSA said:

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

The CBSA also said:

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

You have no basis to dispute any of the things that are said there, do you?

Mr. Evan Light: No, I don't.

Mr. Anthony Housefather: Okay. All I wanted to establish is that I understand. This is really scary technology to a lot of people if it's used improperly, and we need to have safeguards to make sure that it's not used improperly. There are a lot of bad things that can happen, but we have no evidence of that, and I don't want to scare Canadians into believing that's actually happening.

Mr. Evan Light: At the same time, we don't necessarily have any oversight or transparency on the use of these tools, going back almost four years now.

Mr. Anthony Housefather: I mean, again, that's your contention. I would say that we actually do have oversight based on the heads of the departments and the people who, again, are under pretty strong ethical rules to comply, but I get what you're saying. Of course, there are fears, and we have to make sure there are safeguards. Our job as a committee is to make recommendations to make sure policies and regulations are in place to mitigate any concerns that may exist.

Do I have any time left, Mr. Chair?

Mr. Larry Brock (Brantford—Brant, CPC): I have a point of order, Mr. Chair.

The Chair: Go ahead.

Mr. Larry Brock: I'm wondering if Mr. Housefather wishes to become a witness and we can cross-examine him, because he's certainly giving evidence at this—

Ms. Iqra Khalid (Mississauga—Erin Mills, Lib.): I don't think that's a point of order, Chair.

Mr. Larry Brock: He's giving evidence that this committee has not heard through witnesses.

Ms. Iqra Khalid: I'm not sure why we're stopping this—

Mr. Anthony Housefather: I actually just read from the witness testimony—

The Chair: Hold on, Mr. Housefather.

That's not a point of order, Mr. Brock.

Mr. Housefather has the floor and, like all members, he's entitled to give his opinion and his comments and ask his questions. As members of the committee know, members' time is their time.

Go ahead, Mr. Housefather.

Mr. Anthony Housefather: How much time do I have, Mr. Chair?

The Chair: I stopped it at 1:14.

Mr. Anthony Housefather: Thank you.

I appreciate my colleague Mr. Brock's comments. He is probably the person who would be the most verbose in terms of giving his opinions about things, so I am just a little surprised.

Coming back to you, Mr. Light, on a larger question, I understand the many issues you've raised in your literature, and I'm looking forward to getting the translated copies when we get them. We haven't gotten them yet.

If you had one recommendation that you wanted to give to change existing Treasury Board policies or other existing policies, what would it be—your primary one?

Mr. Evan Light: I would say that privacy impact assessments from the Treasury Board should be mandatory in law but also should come before anything is purchased. To date in my broader research, we've asked for around 250 to 300 ATIPs for hundreds of contracts, adding up to about 800 million dollars' worth of purchases related to surveillance. It's a huge amount of money.

Just recently, I got an updated contract from Teel Technologies for mobile forensic devices—the Copyright Board was a new agency that came up as a receiver of these things—for $11 million. It was a recent contract, a renewal. If we're going to be careful with money, we should really ask hard questions about what technology is purchased before it's purchased.

● (1125)

Mr. Anthony Housefather: Thank you.

[*Translation*]

The Chair: Thank you, Mr. Housefather and Mr. Light.

I'm going to ask everyone to speak more slowly, to make things easier for the interpreters.

[*English*]

I didn't know you were an auctioneer, Mr. Housefather. Is that true? No.

If you can, just speak a bit more slowly for the interpreters, if you don't mind. Thank you so much.

[*Translation*]

Go ahead, Mr. Villemure. You have six minutes.

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

Thank you for being here, Mr. Light.

Your research led to an article, and that is why we are here today. We've heard a lot of the same things so far. Officials told us that they had acquired the tool and conducted checks in the past. They said that they had not carried out privacy impact assessments but would. That's the gist of much of what we heard.

Do you think an attitude like that is appropriate when it comes to protecting privacy?

Mr. Evan Light: No.

Keep in mind that I mentioned the normalization of surveillance within government in the CBC article that came out in November.

[*English*]

I think I was quoted here at committee as speaking about what for me seemed to be a normalization of surveillance within government.

[*Translation*]

That's something that worries me. It's as though surveillance is something normal, but it should actually be something that's rare. Privacy is a fundamental right and should be protected by default.

Mr. René Villemure: Most of the witness also told us that they had obtained judicial authorization and had acted within the limits of those warrants. I asked them whether the warrant had replaced the privacy impact assessment, but the answers I got weren't very satisfactory. I felt as though I was asking a pointless question.

Do you think a privacy impact assessment should come before or after a warrant or take its place altogether?

Mr. Evan Light: I think it absolutely has to come before a warrant.

Mr. René Villemure: Should the legislation be amended to require organizations to always start with a privacy impact assessment?

Mr. Evan Light: Yes.

Mr. René Villemure: Very well.

You were talking about the principle of proportionality earlier. In the organizations' search for information, were these the only available tools to obtain the information in question, or was their use too invasive? You touched on proportionality in your opening remarks, but I'd like you to provide more information on that.

Mr. Evan Light: I think that came up when the officials were here. Tuesday, for instance, Scott Jones and Mario Mainville talked about having to balance the violation of employee privacy and the data that are needed or that exist. In their use of the tools, there is an attempt to strike a balance.

Mr. René Villemure: Personally, if I'm using a government-issued device, my expectation of privacy is lower than if I'm using my own personal device, but that doesn't mean I have zero expectation of privacy.

Mr. Evan Light: No, not at all.

Mr. René Villemure: All right.

You talked about the illegal use of cloud accounts by Cellebrite and others. Can you tell us more about that?

Mr. Evan Light: Yes, absolutely, but I'm going to switch to English for the sake of efficiency.

[*English*]

Cellebrite and other companies, for instance—Magnet Forensics does this as well—have the ability to extract what are called “tokens”. When you have apps on a phone that connect to the cloud, you have tokens that essentially log you in. They serve as your unique identity to connect to a cloud service.

In fact, Cellebrite just updated its UFED Cloud, which is being used by at least five or six agencies, so that it can access Lyft and Uber logs. It can access DJI drone flight logs. It can access banking. It can access your Google history, your GPS history.

In the past, you would have needed a warrant for each individual action to access each individual connection to a corporation, and maybe those corporations would have been served with warrants and would have had to provide the information. Instead, now, with a device or an image of a device, this information can be accessed without a warrant.

● (1130)

[*Translation*]

Mr. René Villemure: That is a potential breach of privacy, then.

Mr. Evan Light: Yes.

Mr. René Villemure: I see.

All the witnesses said they got the message and would conduct privacy impact assessments.

Do you think it was negligence on their part, or an oversight? Why didn't they do the privacy impact assessments, in your opinion? I am not trying to criticize anyone. I am just trying to understand what happened. They all said they didn't do an assessment but would going forward. That tells me they recognize it's the right thing to do.

Mr. Evan Light: Had it been just one agency, it would not be as serious. However, it happened everywhere, and that's the problem. The problem is systemic, not just an oversight. Disregarding privacy as a fundamental right is becoming somewhat normalized.

Mr. René Villemure: Perhaps that's the culture of public organizations.

You identified 13 departments and agencies. Have you identified other public organizations since then? Are there more?

Mr. Evan Light: One of the contracts I mentioned a few minutes ago was with Teel Technologies. Recently, I saw that Shared Services Canada had changed its procurement practice. Now, instead of buying the technology directly from suppliers like Cellebrite, it goes through Teel Technologies, a company in Victoria, British Columbia. The current contract runs until the summer of 2024.

The Copyright Board of Canada is also one of the organizations—

Mr. René Villemure: That means there are 14.

Mr. Evan Light: There are more than 13 departments and agencies. I was rather worried when I heard Mr. Jones say on Tuesday that he could purchase the technology for anywhere and anyone. If you're in government, you can place the order and buy it.

Mr. René Villemure: All right. Thank you.

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

[*English*]

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

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

I've taken a note from my good friend René's use of his iPad for timing, so hopefully I'll get it on, although certainly not with the same expediency as my friend Mr. Housefather in the way he was able to deliver questions.

We're well into this. One of the things that typically happen with expert testimony is that they are given time to situate themselves within their subject matter expertise. In your opening remarks, you didn't have an opportunity to do that. I want to give you that opportunity now. I understand, from your profile, that you publish widely on issues of privacy, surveillance and communications. Perhaps, as an opportunity to provide context to that, you can share what expertise you're here with today.

Mr. Evan Light: Yes, happily.

I'm an associate professor of communications at York University's Glendon College. My background is actually in radio spectrum policy, which brought me into surveillance. A lot of the radio waves we use are also used for surveillance. I host an archive of the Edward Snowden documents. For about a decade now, I have been heavily involved in research on surveillance and privacy issues.

Mr. Matthew Green: Would it be your contention that you're here as somebody who advocates for open and transparent government?

Mr. Evan Light: Absolutely.

I also have an IT background. Before becoming an academic, I worked in IT for about 10 years. Ultimately, I ended my career in IT as chief network technician of McGill's Faculty of Law, so I have an understanding from, I guess, the back-end perspective—

Mr. Matthew Green: It's a unique perspective.

Mr. Evan Light: Yes, that's fair to say.

Mr. Matthew Green: One thing that strikes me is that, as legislators here, we're often tasked with trying to propound on technologies and subject matter that we don't have expertise in. I acknowledge that I don't have expertise in the things that you just stated you have expertise in.

While it is true that there are good public servants who, to the best of their ability, are making judgments day to day about the privacy and proportionality of the tools they're using, is it safe to say that the technology you're referencing here would likely go beyond the scope of an average person in government and probably even around this table?

Mr. Evan Light: It's fairly esoteric stuff.

Mr. Matthew Green: And it's sophisticated.

● (1135)

Mr. Evan Light: Yes.

Mr. Matthew Green: It was your contention earlier that one of the red flags—I'll call it a red flag; you didn't say that—in reviewing the companies from which the devices have been procured was that they were actually marketing ways to surreptitiously use backdoor devices to do things that they couldn't otherwise do directly through a warrant. Is that your assertion?

Mr. Evan Light: Yes.

Mr. Matthew Green: That's their own testimony, in fact, by their marketing materials.

Mr. Evan Light: Yes.

Mr. Matthew Green: That is a problem. That is a problem for me, because I do rely on the testimony of people who are here, but I also wouldn't expect them to know all the ways in which the technology they procure could potentially impact their workers or the general public. I reference all the ways in which data breaches happen in high-tech companies, and in fact government, where very sensitive information is shared very widely through malicious attacks.

In your opinion, based on your subject matter expertise, do you have any concerns around the possibility for this technology to be used in ways that might lead to broader breaches in the privacy of individuals?

Mr. Evan Light: Absolutely. I think that talking about its use within or by federal government agencies is really the tip of the iceberg. Nobody, including myself.... I haven't had a chance, to date, to look at this technology among police forces throughout Canada and at every level of government, and there is a high level of possibility of abuse.

Mr. Matthew Green: One of the challenges we have—I would state this as my own opinion—is in terms of the lack of trust and the cynicism in government, and indeed, in some spaces that creeps over into conspiracies. As somebody who is also an open government advocate, would you agree with the notion that greater transparency, greater openness, provides less room for conspiracy or cynicism? In other words, do open governments lead to greater trust in government institutions?

Mr. Evan Light: Absolutely.

Mr. Matthew Green: When you're trying to track procurement—I was also on a file that dealt with government procurement, and I also found it very challenging—can you speak to some of the ways in which you have found it difficult to actually follow what the government is doing? For instance, in previous testimony, you may recall that I asked the procurement director, essentially, of the department what the line item was on the technology, and he couldn't reference it. I also wanted to know what the line items for procurement were related to on-device technology, a.k.a. spyware.

Can you talk about the ways in which it's very difficult, even for somebody with your expertise and your research background, to actually follow the bouncing ball when it comes to tracking exactly what the government is doing, where it's spending money and what it's spending money on?

Mr. Evan Light: Sure. Luckily, I have a research assistant who used to work for the private sector and wrote contracts with the government, so she understands procurement in a way that I do not.

When we do this research, we essentially have a huge list of companies that we know produce really nothing but surveillance tools, and we dig through the open Canada database of government contracts above $10,000. This only gives us access to one or two contracts above $10,000. Anything less than that isn't reported and isn't available to query. Even then, the description of what the contracts are for is very generic. It's hard to actually parse through and see what is being used, unless we find it on ATIP.

To date, over the last three years, we've filed hundreds of ATIPs. Our response rate has been about 37%, so we have hundreds of outstanding ATIPs for hundreds of millions of dollars' worth of contracts.

Mr. Matthew Green: Would that not be solved by proactive disclosure of this stuff, a database that you could just go to and see, rather than having to be forced to search for it through ATIPs?

Mr. Evan Light: Absolutely. I've seen it done elsewhere. For instance, in Uruguay in the 2010s, they were developing really interesting open government technologies where you could see the spending in every ministry and department in real time, and you could track what was happening.

Mr. Matthew Green: That's all. Thank you so much.

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

That concludes our six-minute round. We are going to go to our five-minute round and start with Mr. Brock.

Go ahead, Mr. Brock.

Mr. Larry Brock: Thank you, Chair.

Good morning, Professor.

I want to focus not on the device itself and the software attached to it—which is the focus of this committee hearing—but rather on the broader issue of privacy. You spoke in general terms about this being a fundamental human right. It has been a fundamental right in Canada since 1977.

I'd like to get your expert opinion, sir, on the disastrous ArriveCAN app, which has just been revealed to be an abuse of taxpayer dollars of over $60 million.

Think back, if you can, to the time when the ArriveCAN app was heavily promoted by this government. It was the way to go in terms of dealing with COVID and trying to protect Canadians, etc. There's a portion in the preamble when you sign up for the ArriveCAN app that I'd like your opinion on. The title is “How your information is used and disclosed”. It says:

> Personal information may be disclosed to contractors working for the Public Health Agency of Canada and Service Canada as well as to the following entities: other government institutions, as well as provincial, territorial, municipal governments or international health organizations as well as their institutions for these purposes.
>
> Personal information may also be used for program evaluation. In other limited and specific circumstances, personal information may be used and/or disclosed without consent in accordance with section 7 and subsection 8(2) of the Privacy Act.

It looks like tens of millions of Canadians who were forced by the Trudeau government to sign up for the ArriveCAN app had their personal information wildly—

● (1140)

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

The Chair: Hold on, Mr. Brock. There is a point of order.

Go ahead, Ms. Khalid.

Ms. Iqra Khalid: Thanks, Chair.

I'm just questioning the relevance of Mr. Brock's questioning. I'm sure the witness was not called for the line of questioning that Mr. Brock has delved down.

The Chair: Just hang on a second. In every circumstance where a point of order is made, I am consistent in my ruling. I did it with Mr. Housefather, and I'm doing it again with Mr. Brock.

It's his time. We have a subject matter expert on privacy who is before us here. I am going to allow Mr. Brock to continue. He has the floor, and I'm sure he's going to bring this to where it needs to go.

Mr. Brock.

Ms. Iqra Khalid: Just to clarify—

The Chair: Ms. Khalid, we can beat a dead horse on this. I've been chair of this committee now for almost a year and a half, and my rulings have been consistent in every circumstance for every member who sits around this table.

Mr. Brock, you have three minutes and two seconds. Go ahead.

Mr. Larry Brock: You heard the exchange. Some Liberal members don't care about privacy. Conservatives certainly do.

Ms. Iqra Khalid: I object to that.

The Chair: Mr. Brock, it's a matter of opinion.

Ms. Iqra Khalid: Chair, I wasn't going to say it, but I will say it now. Mr. Brock started his questioning by saying that he's going to be asking questions that are not relevant to the topic at hand today.

The Chair: I'm not sure I heard him say that, but I can certainly check back.

Mr. Brock, you have the floor for two minutes and 50 seconds.

Mr. Larry Brock: It's all about privacy.

Professor Light, can I get your opinion on what I just read out to you? Is that a danger? Was that a danger?

Mr. Evan Light: Sure. I just want to preface this by stating that I am a member of no political party, and I come to this believing that privacy is a completely non-partisan issue. We're talking about a human right.

Mr. Larry Brock: Yes.

Mr. Evan Light: It's not negotiable. It's not debatable.

I think the preamble you read is really fascinating because to me it speaks to—if you remember—Bill C-51, which was a Harper government law that created a brand new level of data sharing between government agencies.

The preamble sort of lays out how that happens. It shows you how this information flows between agencies and how it has become quite a normal thing to do. That dates back a very long time. It's not a new thing. It has probably been going on since before the Harper years, but I think it's something that maybe was informal and now has become quite formalized.

It does scare me. As somebody who used ArriveCAN when it came out because I found it easier—I wasn't provided with paper on a plane to fill out—I think that our technologies at airports and borders are quite invasive. They're also quite invasive everywhere in the world. I've been to airports in Europe where I couldn't get a connection without having my face and my hands scanned.

I think our levels of invasion are not necessarily at that high level here, but yes, I think it's problematic.

Mr. Larry Brock: Particularly with the phrase “without consent”, I think it is extremely problematic.

Would you agree with that?

Mr. Evan Light: Yes, and I think that the position it puts a traveller in, for instance, just as in the case of using mobile forensic devices within agencies for administrative purposes.... You're in a position where you can't necessarily consent, where there is a power imbalance, so you are doing something because—

Mr. Larry Brock: One can only surmise what type of information is in the possession right now of the Government of Canada that is not used for the purposes of protecting that individual from COVID.

Another issue I want to discuss....

How much time do I have, Chair?

The Chair: You have 45 seconds, Mr. Brock, and I'm sticking to the timelines.

Mr. Larry Brock: Thank you.

You're aware that the Auditor General released a report. She talked about cybersecurity leaks and the individuals, the contractors, not having proper security clearance.

How do you weigh that, sir, in terms of an opinion?

Mr. Evan Light: I can't say. I haven't read it closely.

Mr. Larry Brock: You have not.

Mr. Evan Light: No.

Mr. Larry Brock: Okay. It says, “Although the agency told us that the resources did not have access to travellers’ personal information, having resources that were not security-cleared exposed the agency to an increased risk of security breaches.” This is in relation to the CBSA giving contractors without security clearance the authority to gain information on travellers.

What's your opinion on that, sir?

● (1145)

Mr. Evan Light: I would say that's problematic.

The Chair: Thank you, Mr. Brock.

Ms. Khalid, go ahead, please.

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

Thank you, Mr. Light, for being here today.

The member for Brantford—Brant recently said in the government operations committee that if people are public servants, there are no privacy issues.

Do you believe that public servants are entitled to privacy?

Mr. Evan Light: Yes, and if you look back a few weeks ago, Brigitte Bureau at Radio-Canada published an article exactly on this issue and interviewed two legal experts. I am not a lawyer and I don't consider myself a legal expert, but one law professor and one lawyer both said that employees, civil servants, do have an expectation of privacy and do have the right to privacy even when they're using government-issued devices. There is a difference between the device itself and the stuff on the device.

Ms. Iqra Khalid: When a government employee, for example, is given a device that they use for their work, which is what we're talking about in these 13 departments, do they have a reasonable expectation of privacy on those government phones, which they use and which were given to them to be able to do their work better?

Mr. Evan Light: I believe so.

Ms. Iqra Khalid: With that reasonable expectation of privacy and the consent piece of it, what is the role that a privacy impact assessment plays in how departments manage their relationships with their employees?

Mr. Evan Light: Right now I think privacy impact assessments are not necessarily a standard thing. They push an agency through a line of questioning that helps them think about how to meet this balance of privacy violations and privacy protections.

However, that process isn't necessarily clear, I don't think, to employees. I think it's there for guidance at a high level, but it's not there for understanding at the ground level.

Ms. Iqra Khalid: To be clear, employees' personal phones are not impacted by what we are talking about today. It is specifically government-owned devices. Is that correct?

Mr. Evan Light: I think the committee has spoken about a number of different possible uses. There are uses in administrative cases for internal evaluation of government-owned phones, and then most of the organizations that you've had testify to you have spoken about the use on devices of non-employees. DFO, Transportation Safety Board, CBSA, the RCMP use this on non-employees as well.

Ms. Iqra Khalid: I'm not sure if that was my take on the testimony that we heard.

However, just on that, the relationship between warrants and hypotheticals, as in what could be done or what is possible versus what is actually done.... Do you think there is a break in public trust? Clearly you have mistrust in how departments are operating these devices with their employees. How do you think we can work to build better trust so that you and others don't think that what could be done is actually being done?

Mr. Evan Light: For me, as a researcher, I want clear evidence.

In the process of preparing ATIPs for these agencies for their internal policies, for their use logs, it's about this: Show me what you use these things for; show me why you use them; show me what policies exist and what policies don't, what laws exist and what laws don't.

Ms. Iqra Khalid: My understanding is that all of whatever is done to employee phones is done either through consent or through warrants. Do you think that is not sufficient to protect an employee?

Mr. Evan Light: I don't think consent is enough. I don't think people necessarily know what they're consenting to.

Ms. Iqra Khalid: If consent is not enough, then what is?

Mr. Evan Light: We go back to my comments around privacy impact assessments being tools for self-regulation. We need to have an external body like the OPC that decides whether or not these things should be used in the first place. A body like the OPC could decide what sort of processes need to be in place for people to give informed consent around the examination of their devices.

Ms. Iqra Khalid: Do you hold that same view for private organizations as they deal with their employees, or is it just government departments that you feel need to go through these extra measures?

● (1150)

Mr. Evan Light: Do you mean corporations?

Ms. Iqra Khalid: Yes.

Mr. Evan Light: I would be troubled if corporations were able to buy these technologies. If they were, I would have the same expectations in terms of consent.

Ms. Iqra Khalid: Lastly, I just want to go through what your definitions were with respect to spyware and digital forensic software. You said that they are basically one and the same, but that's not what we've heard in testimony from other witnesses. Can you clarify your position on that, please?

Mr. Evan Light: Their capabilities are somewhat the same. With spyware, you have applications that are surreptitiously installed on people's phones in order to spy on them in real time. Mobile forensic devices give you the ability to access the same granularity of data after the fact, so they're not the same thing at all, but they essentially provide the same access to data that you would not have otherwise without having to get a warrant, to the degree that you would need to get a warrant to access each connection to a cloud service provider, for instance.

Ms. Iqra Khalid: You don't have evidence to support that this is what is actually being done in these departments for now.

Mr. Evan Light: No, but I do have evidence that they have purchased the technology to do it. Why would you purchase technology to be able to access these things if you were not planning to do it? These are separate technologies. Mobile forensic devices are various software and hardware pieces. They can be bought piecemeal, and technology with the capability of doing this has been recently purchased. There are licences that are active through the middle of summer 2024.

The Chair: Thank you, Mr. Light.

Thank you, Ms. Khalid.

[*Translation*]

It sounds like someone's phone is making noise. Could you please put your phones on silent mode?

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

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

Mr. Light, the things you're describing are quite worrisome. Technology moves quickly. Some organizations come back to the fact that, back in the day, hiding a microphone in a lamp did the job, but today, they have to use forensic technological tools. Given how far technology has come, is a privacy impact assessment enough?

Mr. Evan Light: I don't think so.

The comments the committee has heard so far all point to the same concern, a privacy impact assessment examines the program, not the technology. As the Competition Bureau Canada officials told the committee on Tuesday, this type of tool has been in place since 1996, before the Treasury Board directive was introduced. Other organizations such as Shared Services Canada have privacy directives that predate the use of these tools. It's wrong to think that the data are the same as they always were. More and more data are available thanks to these new technologies.

Mr. René Villemure: Do you think the Privacy Commissioner is going to have to keep a more watchful eye on things given how far the technology has come?

Mr. Evan Light: Yes, absolutely.

Mr. René Villemure: All right.

You mentioned the comments of other witnesses a number of times. Were you reassured by what you heard the witnesses say this week? Is everything going to be fine?

Mr. Evan Light: No.

Mr. René Villemure: No?

Mr. Evan Light: I'm reassured because I now know a lot more about what's going on than I did before.

Mr. René Villemure: Would you say that the whole reality around privacy, to some extent, amounts to underestimating its value?

Mr. Evan Light: I think so. With our use of technology, social media and new ways of communicating, we developed new social standards and new communication standards, but we haven't updated our laws.

Mr. René Villemure: Does privacy exist anymore?

Mr. Evan Light: I think so, but it's at risk.

Mr. René Villemure: All right. Thank you.

The Chair: Thank you, Mr. Villemure.

[*English*]

We'll go to Mr. Green for two and a half minutes. Then we'll go to Mrs. Kusie for two and a half minutes, and then Ms. Damoff. That will complete the round.

Mr. Green.

Mr. Matthew Green: Thank you very much.

I think one challenge we have is that we're only ever in these committees having these discussions kind of after the fact. We know that with the on-device technology the RCMP was using, there was no proactive disclosure there. It took some revelations around procurement for us to find that out. Now we're here in the same boat.

Going back to our earlier conversations about finding and pinpointing key recommendations to this committee, with your experience on access to information and on procurement, what are some ways that we can create a culture of proactive disclosure so that people have a better understanding of what the government is doing?

● (1155)

Mr. Evan Light: If we go back to the model where the OPC would have a role in procurement, then we'd have a reporting mechanism. Instead of having agencies making up their minds about what they do on their own, there's an obstacle there. There's a step that everybody has to pass through where information becomes public and where a committee like this could be asked to review a certain technology before it's used. Right now, it's really all pretty piecemeal.

Mr. Matthew Green: Yes, it's very piecemeal. We heard that as a consistent reflection from the departments. Each of them was picking and choosing its own adventure. Some of them were saying they had various forms of a privacy impact assessment. I also picked up that some of them were not assessing the actual tool, but their “programs”.

Why do you think it would be a problem to have a PIA on a program rather than the specificity of the tool?

Mr. Evan Light: Tools change all the time and their abilities change all the time. The programs are probably too general to capture the evolving capabilities of tools.

Mr. Matthew Green: In your opinion, having a broad look at this entire sector of technology, is it safe to say that in both the private and the public sector, this is a completely unregulated field?

Mr. Evan Light: Absolutely.

Mr. Matthew Green: Is it safe to say that in light of disinformation, misinformation and the ability for surreptitious surveillance to create profiles that form algorithms, both in the public and in the private sector, we need to have a framework in place that safeguards Canadians' data sovereignty?

Can you comment a bit on data sovereignty as an effective means for protecting our democratic institutions?

Mr. Evan Light: I couldn't say whether or not data sovereignty is out of the scope of the conversation. I think that—

Mr. Matthew Green: I just put it in the scope of the conversation. What's your opinion on data sovereignty?

The Chair: We're going to need a very quick opinion, please, or you can put it in writing.

Mr. Evan Light: I'll put it in writing.

The Chair: Okay, it's the same thing. Submit it by one week from today at five o'clock, if you don't mind, Mr. Light.

Thank you, Mr. Green.

[*Translation*]

We now go to Mrs. Kusie for two and a half minutes.

[*English*]

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

Thank you, Professor Light, for being here today.

Given your concerns about the lack of transparency and oversight by the current government, are you concerned when the President of the Treasury Board, the person who's supposed to be responsible for enforcing these privacy impact assessments, states that it's the job of each institution and each department to enforce this compliance themselves?

Mr. Evan Light: Yes, it's a problem, but I don't think it's necessarily limited to the current government.

This directive actually originates in 2002. This was misstated by various witnesses at this committee, who were basing this on the 2018 directive. The original directive was in 2002. I think it's been ignored since 2002.

Mrs. Stephanie Kusie: Further to your comments about oversight and transparency, we are running into this problem in our study in the government operations committee. For example, we have the individual who recently conducted the internal investigation, the executive director of professional integrity, reporting to the head of the CBSA.

We've recently seen two data breaches within the government. On November 18, 2023, it was reported by CTV that the information, both personal and financial, of the RCMP and the Canadian Armed Forces was compromised, with this breach going back as far as 1999. Second, just a few days ago, on February 12, it was reported that a subcontractor of Canada Life also had their information breached. These are two very specific examples relative to both public servants and government agencies.

Would you say that the cloud environment and these tools that you mentioned provide for a greater possibility for more breaches like these?

Mr. Evan Light: Yes, definitely. For instance, if government information is on the cloud and people access it through the cloud on a device, then that could be a possibility.

Mrs. Stephanie Kusie: Excellent.

You stated recently that Canada has entered an era of "normalization" of surveillance. Can you expand specifically beyond that, please?

Mr. Evan Light: Sure. I don't think we've entered it; I think it goes back a very long time. For instance, in my work looking at how we use radio waves to do surveillance in Canada, CSIS has had the authority from, at that time, the Department of Communications to use the airwaves to surveil domestically since 1991.

I think surveillance is something that will always be within and outside of government. I don't think it's necessarily that surveillance has become normalized. I think it's [*Inaudible—Editor*] that it's used. I think the lack of regulation and transparency around it has become normalized.

● (1200)

Mrs. Stephanie Kusie: Thank you.

Thank you, Chair.

The Chair: Thank you, Mrs. Kusie and Mr. Light.

Ms. Damoff, go ahead for two and a half minutes.

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

Thank you to our witness for being here today.

I wanted to talk a little bit about the use of work phones. I've mentioned this previously. In 1996, in the days before we even had cellphones, I was working at Midland Walwyn. I had to sign something that said my work computer was to be used for work only.

When we talk about consent, I think employees should have a good sense that the work phone that they're given is to be used for work purposes only. Would you agree with that?

Mr. Evan Light: I would, but with the caveat that as technology advances, we see a really big merger of the private and the professional.

Ms. Pam Damoff: I'm not saying that people don't use it for private reasons, but there is an expectation that your employer, whether you work for the government or whether you work for an investment bank, is giving you a tool to help you with your job, not to allow you to do something out of work.

I want to share with you some of the testimony we got previously from Shared Services Canada. The witness said, "while the initial media coverage referenced spyware, I want to assure you that under no circumstances is this an accurate description of the tools used by SSC."

They also said:

> Investigations happen only when there's a credible allegation of employee wrongdoing and to ensure the security of government networks upon which Canadians depend. Impacted employees are always made aware of the conduct of these investigations, and procedural fairness is ensured.

We heard similar testimony from CBSA, where there's only a warrant. It's not when they take your phone during a secondary screening. It's only when they have a warrant.

Then the RCMP said, "The media reports suggesting that these digital forensic tools are considered spyware are inaccurate...and I will clarify". He said, "These tools are used on digital devices that are lawfully seized through criminal investigations."

I guess my question is this: Do you think these people are telling the truth when they come to committee to say these things?

Mr. Evan Light: I believe they're telling the truth, but I believe the law and the policies have not kept up with the capabilities of these devices and what they're capable of.

Ms. Pam Damoff: Okay. That's fair.

Mr. Evan Light: I don't believe employees understand that.

Ms. Pam Damoff: Well, I think employees have to take some onus on themselves when they're doing something for work. I also think that if there's a suggestion of harassment or wrongdoing by the employee, regardless of where you work, your employer should have the ability to use the proper legal tools, including with your phone, to investigate allegations of wrongdoing.

My time is up, Chair. Thank you.

The Chair: Thank you, Ms. Damoff.

Mr. Light, I want to thank you for appearing before the committee today with your testimony.

The next panel needs to be set up, so we'll suspend for a couple of minutes. We'll be back soon.

Thank you.

● (1200)

_____(Pause)_____

● (1210)

The Chair: Welcome back for our second hour. That took a little longer than a couple of minutes, but let's get started here.

Welcome to our witnesses for the second hour today. From the Canadian Association of Professional Employees, we have Nathan Prier, president, and Laura Shantz, senior adviser, advocacy and campaigns. From the Professional Institute of the Public Service of Canada, Jennifer Carr is here.

I want to welcome all three of you and thank you for being here today. You have up to five minutes to address the committee.

We'll start with the Canadian Association of Professional Employees. Go ahead, sir.

Mr. Nathan Prier (President, Canadian Association of Professional Employees): Good afternoon, and thank you for the opportunity to appear before the committee today.

My name's Nathan Prier. I'm the president of the Canadian Association of Professional Employees, where I represent over 25,000 public sector workers in the economics and social sciences services and translation groups, as well as employees of the Library of Parliament, the Office of the Parliamentary Budget Officer, and civilian members of the RCMP.

We're shocked and dismayed to learn that spyware has been used in multiple federal departments, on federal devices used by public sector workers, without following the government's own policies. The use of this spyware was uncovered, as we just heard, through an access to information request submitted by Dr. Light, and public sector workers learned of the potential breach of their rights from the press instead of through mandated privacy assessments or any sort of proactive disclosure by the employer.

This kind of secretive behaviour damages the trust between public sector workers and their employer. Dr. Light described the use of this spyware as "overkill" and "ridiculous, but also dangerous", and we just heard some examples of why he feels that way. In our estimation, the use of such software is pretty heavy-handed and is a breach of our members' trust.

The government's directive on privacy impact assessment is in place to ensure that any data collection is done through the least intrusive methods possible, and the government's own Privacy Commissioner has indicated that assessments are warranted whenever privacy-infringing tools are used, even when there is judicial authorization in place that some measure be used. The 13 departments in question here didn't perform privacy impact assessments before using this spyware, despite their own policies requiring such an assessment to be done, and for us that's completely unacceptable.

[*Translation*]

Federal public sector workers should enjoy the same rights to privacy and due process as all other Canadians. Their employer should treat them in a way that builds trust, so that they can deliver quality service to Canadians. In order to rebuild this trust and ensure that government workers maintain their rights to privacy and due process, we call on the federal government to make a plan to update and consistently follow its digital policy framework.

● (1215)

[*English*]

CAPE, my union, is here to present three specific requests.

First, we're calling on the government to stop the use of spyware on federal devices outside of its own established rules, and to use the least invasive measures necessary. All public sector workers deserve due process during investigations.

Second, we want to know when the government plans to conduct privacy impact assessments at all affected departments and to publicly release the results of these assessments to help public workers rebuild trust in their employer after these breaches. Spyware use represents an erosion of privacy rights that no public worker should accept on its face.

Finally, we call on the government to conduct a thorough review of all its digital policies to ensure that the existing policy framework is adequately robust to protect employees' digital rights, including their right to reasonable privacy, their right to be informed about any digital surveillance tools being used in the workplace and their right to disconnect from work at the end of the day.

CAPE members deliver sound policy advice for the government, and they can only do their best work when the employer demonstrates willingness to be open, transparent and respectful of the public sector.

The Chair: Thank you, Mr. Prier.

Ms. Carr, you have five minutes. Go ahead.

Ms. Jennifer Carr (President, The Professional Institute of the Public Service of Canada): Thank you, Mr. Chair.

Thank you for the invitation to speak with you today.

My name is Jennifer Carr, and I'm the proud president of the Professional Institute of the Public Service of Canada. We represent 75,000 federal public servants and some in the provincial sphere as well. We also represent IT workers.

I want to start today by making our position very clear. Employees' privacy rights must be protected. Government employees, our members, are Canadian citizens just like you and me. We all have the right to know when our information is being accessed, what information is being gathered, how it's going to be used, who has it and who will have access to it, and how it's being stored and protected. I hope we can all agree that, as one of the largest employers, the federal government should set the example for all other employers and be held to the highest standard.

Sadly, as you have heard, it appears that many government departments and agencies have not done so. They have failed to abide by the government's own policies and rules. They've apparently disregarded the Treasury Board directive requiring that privacy impact assessments be carried out before using these kinds of tools.

We're talking about federal departments and agencies potentially using these tools to obtain access to text messages, emails, photos and travel history, to access cloud-based data and reveal Internet search histories, deleted content and social media activities, and possibly to recover encrypted or password-protected information.

Think about all the information that you have right now on your phone, your tablets, your watch or your computer: health data, financial information, deleted messages from friends and family, or cloud-based information like your family photos stored on Dropbox, Google or OneDrive. The idea that using an employer-supplied phone or computer means that you are giving up all your rights to privacy is absurd.

We are deeply concerned to learn that some employers, like Fisheries and Oceans Canada, claimed that the use of these tools was justified because the data belongs to the department.

Your employer may own the device, but that does not mean they own your personal data on it. The Privacy Commissioner and legal experts have been crystal clear on this. The commissioner also made it clear that, even when there is a legal authorization, it doesn't mean that the departments are exempt from doing the privacy impact assessment. These assessments are critical to identifying potential privacy risks and figuring out how those risks can be mitigated and/or eliminated.

The Privacy Commissioner should make it clear that his office must be consulted before these tools are used, and not learn about it in the media stories after the fact.

We also need transparency around how often assessments are required to be done and what should trigger one if we need to do a new one. Technology is evolving at a rate faster than we've ever seen before. This means that our privacy laws, regulations and practices need to evolve just as fast.

Moreover, government departments and agencies should be required to consult the Privacy Commissioner prior to adopting any new privacy rules, especially when they pertain to the use of intrusive software tools. Failing this, MPs should amend the Privacy Act to make this a requirement under the law.

The employees we represent are also concerned about the testimony you have heard by some of their departments. Health Canada first said that they had purchased but never used these tools, before admitting that they had used them, but wouldn't say for what. Defence officials testified that it was unclear whether the privacy impact assessments were completed or not. RCMP officials told you that they were using the tools, but would only do the impact assessment later this year.

As the union representing tens of thousands of federal employees, these mixed messages heighten our concerns about electronic surveillance in our workplaces.

In closing, I want to thank you, committee members, for launching this study. Our members appreciate your decision to look into this issue. We urge you to make strong and clear recommendations on how government employees' personal data should be better protected. These recommendations should include the following.

Government departments and agencies should be required by law to conduct privacy impact assessments before using any of these tools, regardless of whether legal authorizations exist, as the Privacy Commissioner recommended, and less intrusive methods should be used to gather information, as required by the privacy impact assessment directive.

● (1220)

When departments and agencies fail to abide by Treasury Board directives, there should be clear repercussions and actions to ensure that they have further compliance.

The second is that clearer guidelines be provided around what new or modified programs will require new privacy assessments and that current ones be updated. Technology is moving at a fast pace, and our practices need to reflect that reality.

Finally, the government must acknowledge that the use of an employee's device does not give it ownership of people’s personal data on it. As the tools that this study has been asked to investigate become more powerful and invasive, privacy protections must be improved to keep pace.

We urge all MPs to come together to ensure that the government maintains the highest standards when it comes to employees’ privacy. Let’s make our government a shining example as an employer across the country when it comes to protecting privacy in the workplace.

Thank you.

The Chair: Thank you.

I want to thank both of you for your opening statements and, more so, for providing solutions. It's not often that we have witnesses who come with these types of solutions and recommendations to the committee, so I appreciate that you both have done that.

Mr. Kurek, you have six minutes in the opening round. Go ahead, please.

Mr. Damien Kurek: Thanks very much.

Thank you to our witnesses for being here.

Now, I want to pre-empt what seems to have been the argument from the government on a number of cases. First—and it addresses this specifically, so I want to give you a chance to answer this—the government has said, “Oh, don't worry. It's not spyware.” It's troubling because these are incredibly powerful tools that have access to that personal information.

I'll direct that question to Mr. Prier. However, I'll ask my second one as well, which will be for Ms. Carr. It's surrounding the fact that it's a government device and, therefore, you basically have no rights. That's a paraphrase of even the questions that we heard from a parliamentary secretary in the last hour, and I think you were here for that. So, I'd like to ask for your opinion on that and whether you could provide some context as to why you referred to it as those things in your opening statement. Then I have a couple more questions that I'd like to get to.

We'll start with Mr. Prier.

Mr. Nathan Prier: I would say that whether or not we call it spyware, by definition—we could argue over the definition—it is technology that is infringing on our members' privacy rights. I think that's the basic line that was crossed here.

The proactive disclosure of the use of this technology, even though the Treasury Board directives state that this should have happened, did not happen. We learned about it after the fact.

I'll just speak to the issue of whether the fact that it's a government device means that it's able to suspend all members' privacy rights as such. The federal government is one of the biggest employers in this country. It needs to be setting a high bar and a high example for how we expect all employers to behave toward all Canadian citizens and their privacy rights as such. We feel that, in this case and in many other cases, it seems that we're slowly learning that basic policy wasn't followed.

The Privacy Commissioner was very clear that when new tools are developed that pose privacy risks, as we've seen here, this merits a privacy impact assessment and proactive disclosure. I think there are very easy ways to communicate proactive disclosure of these technologies in plain language that will make workers in a workplace, our members, federal public servants, much more able to not just abide by basic standards of what is to be shared on a government device but be aware of their privacy rights and the potential violations of them, so that this discussion can happen before these technologies are installed.

● (1225)

Mr. Damien Kurek: I hate to cut you off, but as you know, we have limited time.

You may have heard my not-so-subtle advice to department heads and whatnot to pick up the phone and call the Privacy Commissioner. It needs to be done so that we can start to restore that trust, both with Canadians and with the hard-working men and women in our public service.

Ms. Carr.

Ms. Jennifer Carr: I'll be concise.

You may not know that there is already a policy on using digital devices. In that policy, it says that you can actually use the government devices for personal use if it does not interfere with your work, if it is done on your own time. I'm not sure that this was brought up before by anyone else.

There are a lot of policy suites that exist within the government sphere, but as we leave them to be decentralized and applied by individual departments instead of centralized through Treasury Board and oversight, that's where we get into trouble.

Mr. Damien Kurek: I appreciate that. I think it's important, especially because cellphones and mobile devices have become such powerful communications tools. No longer are they just a cellphone or just an email device. They're so much more than that.

I am curious—and I want to hear your opinion first—if you could offer any examples of when these investigative tools have been used to find whistle-blowers or people who have been targeted because of their actions within a particular department. Specifically in terms of finding a whistle-blower, I'm wondering if there are any examples—if you've heard that or can cite them. I'd also just ask for your opinion about how this could infringe on a worker's ability to call out what could be misconduct within the department, agency or otherwise.

Ms. Jennifer Carr: One thing that concerns me about some of the testimony is that they say they have the software but they don't use it; they send it off to another department. If the technology exists and we don't know how it's being used, and if they don't have to disclose when and how it's being used, that's very concerning.

I can't point to a specific example, but having technology and not having any kind of disclosure on when you need to use it, any director or DG signing off, that is very concerning. No oversight means it can be used without us knowing.

Mr. Damien Kurek: Mr. Prier, was there anything you wanted to add to that? There's about a minute left.

Mr. Nathan Prier: No, I just wanted to say that I agree with Jennifer on the points that she made. Also, the employer has a strong track record here of being reactive instead of proactive when it comes to digital policy and privacy. A lot of Treasury Board policies are in desperate need of updating for the digital world and probably need to be constantly refreshed as we go.

I think the policy framework we have is strong enough; it just needs to be followed more closely.

Mr. Damien Kurek: I appreciate that. The proactive versus reactive, that's the message I think it would behoove the government departments to follow.

When it comes to the use of these tools and the idea of consent by employees, we heard in testimony from the last hour about the power imbalance.

Can you provide brief context?

Ms. Jennifer Carr: That's a great question.

Because of when these policies were put in place.... What is the consent? I don't think that when the original policy.... When it was just your cellphone, they would have access to whom you'd called and for how long. They haven't done it, when we're using these tools, for cloud-based things. These tools will allow you to go into those clouds. They will allow you to go into encrypted, password-protected...they have all your history.

That was not contemplated way back. We need to have updated policies. I hope you can agree that with the unlimited potential for them to use this tool to find anything, it's absurd that we would think that they [*Inaudible—Editor*] privacy.

The Chair: Thank you, Ms. Carr.

We did go a little over. I'm trying to keep the tight timelines, respecting everyone's time.

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

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

Thank you to our witnesses for joining us today. Thank you for sharing your recommendations. Part of our work as a committee is to make recommendations. Thank you for sharing those off the top, from both organizations.

We did hear from the Privacy Commissioner about the use of the term “spyware” specifically. This is a quote from the testimony the Privacy Commissioner gave us. He said, “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.” He also said, “Digital forensics tools are distinct from spyware in that spyware is typically installed remotely on a person's device without their knowledge.”

We've heard that these devices are used within regulations, a warrant, and the knowledge of employees. We've heard from several agencies when we asked them about.... I think I specifically asked if you can remotely access people's information with these tools and they say, no, you have to get a warrant and physically obtain the device, connect to it, and then you can extract the information that we've been talking about.

Do you have any thoughts on that, Ms. Carr?

● (1230)

Ms. Jennifer Carr: We have this testimony, but it's not clear. Every department has come in and given you a different version of how they're using it. If it is true that you're handing your device off to a third party, why do the departments actually buy and procure this software and have it in-house? I have some concerns about the testimony that they've given that it cannot be done remotely.

The other thing is, what are they pulling? Can they pull everything? Is a warrant all-inclusive or are they specifically gathering certain information?

Mr. Parm Bains: We did hear from several agencies that are investigating something. Many of them have an enforcement piece to those departments. It would be specific to what the investigation is, and the warrant would be specific to that. They would only be able to obtain the information specific to whatever the investigation is. That was the testimony that we heard.

Are employees made aware when using these devices that they are for professional use and not personal use? For example, we have two devices.

Ms. Jennifer Carr: Again, I referred to a policy. I will get you the actual name of the policy, but it does say that work devices can be used for personal use if it doesn't interfere with the work they are doing, if it's done on personal time. The misconception is that it is only an employer device. It is encouraged by certain departments—and it has been for a long time—that you can use your work devices as personal devices as well.

Mr. Parm Bains: Is it outlined to employees in advance that for your professional device the information on there can be looked at?

Ms. Jennifer Carr: I don't believe so.

Again, when I talk about decentralization, each department that hands out these devices would be responsible for making those disclosures, and it's not done in a consistent manner that is gathered at the higher level.

Mr. Parm Bains: Would it be helpful if it were at that level?

Ms. Jennifer Carr: It would be helpful if they made those disclosures, but again, if a policy says that you can, we really need to specify and drill down on what information would be gathered from your phone if under an investigation.

Mr. Parm Bains: I think we've heard from you that you believe in a correct balance between security and privacy, that there needs to be that measure in place. We've also heard that departments use this software for internal investigations and cite reasons like allegations of employee wrongdoing and instances of sexual harassment. Do you believe that this use is warranted?

Ms. Jennifer Carr: Yes. I do believe that, when investigating that, you should be using tools, but it should be very clear to the employee what you will access. I don't believe that the policies right now are clear that they could go and search in your back history and delete it and encrypt it and stuff, so I think more disclosure, more transparency and more accountability on both sides would be beneficial.

Mr. Parm Bains: What percentage of public servants receive government-issued devices?

Ms. Jennifer Carr: That I can't tell you. That would probably be a question for the departments. There is no consistent policy on who can access that. It is really on an individual basis that they are issued.

● (1235)

Mr. Parm Bains: Has there been a level of privacy set that's expected for government-issued devices?

Ms. Jennifer Carr: I don't believe so.

Mr. Parm Bains: Thank you for your time.

The Chair: Thank you, Mr. Bains.

[*Translation*]

We now go to Mr. Villemure for six minutes.

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

I'm going to take this opportunity to give notice of a motion.

The Chair: Very well.

Mr. René Villemure: The motion reads as follows:

> That, in accordance with section 108(3)(h), the Commitee undertake a study of the ethics and compliance with the rules of professional conduct in the awarding of contracts entered into by the government and the companies GCStrategies and Coredal systems consulting inc, with regard to the ethical obligations arising from the Code of Values and Ethics for the Public Sector;
>
> That the Commitee allocate a minimum of four meetings to this study;
>
> That the Commitee invite to testify :
>
> (a) Jointly, for two hours, Anita Anand President of the Treasury Board and Jean-Yves Duclos Minister of Public Services and Procurement Canada, as well as public servants;
>
> (b) For two hours, the President of the Canada Border Services Agency, Erin O'Gorman, and public servants;
>
> (c) And any other witnesses the Committee deems necessary.
>
> That the Committee report its observations and recommendations to the House.

The motion was sent to the clerk in both official languages.

The Chair: Thank you for that notice of motion, Mr. Villemure. I gather that the motion has been distributed to the committee members.

You have four minutes and 45 seconds left.

Mr. René Villemure: Were you surprised, Mr. Prier, when you heard about this practice?

Mr. Nathan Prier: We were surprised that the policies in place weren't followed. We were surprised that the values underlying those policies were completely disregarded.

Mr. René Villemure: I see.

Mr. Nathan Prier: However, we weren't surprised that the employer had installed the tools without discussing it.

Mr. René Villemure: All right.

Were you surprised, Ms. Carr?

[*English*]

Ms. Jennifer Carr: I wasn't surprised. I'm disappointed but not surprised. As we have decentralization of the federal public service, this is common for most of the violations that we see. There's little oversight in departments on some of these policies, and we need to have better oversight.

[*Translation*]

Mr. René Villemure: Were you reassured by the answers given by the officials who have appeared before the committee thus far?

[*English*]

Ms. Jennifer Carr: Absolutely not.

[*Translation*]

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

[*English*]

Mr. Nathan Prier: No. We expect much more in the future.

[*Translation*]

Mr. René Villemure: I see.

The officials who appeared before the committee said that they were using the tools, that they had had them for a long time and that they were going to carry out privacy impact assessments. I think we were surprised to hear them say that they were going to do the assessments. We'll see if they end up doing them.

Do you think that's a way to downplay the situation, that they were negligent? Is it a problem with the corporate culture, do you think?

[*English*]

Mr. Nathan Prier: I think this is a government-wide problem. I think there needs to be strong direction from the Treasury Board to explain exactly how privacy policies are going to be actually implemented in practice.

With that in mind, any new technology that's being rolled out that will impact our members' privacy requires these privacy impact assessments and these proactive disclosures. It's fairly clear in the directive and it's fairly clear in the Privacy Commissioner's statements what is needed here.

Whether it's installed remotely, whether it's installed—

[*Translation*]

Mr. René Villemure: The directives were already in place, though.

[*English*]

Mr. Nathan Prier: Right.

[*Translation*]

Mr. René Villemure: The directives were not followed. I don't know what's going to happen.

Ms. Carr, do you think it's a corporate culture problem?

[*English*]

Ms. Jennifer Carr: It definitely is.

Again, when we have departments that can decide what to do on their own without any kind of oversight, if we're not watching, then they're not doing.

When it comes to the privacy assessment, I did hear, “Well, they said we did one way back.” I would say that we need to update things, so that when new versions come out and new technology comes out, we start to use them. I equated it to saying that we're still subscribing to Napster when everybody is now on Spotify or Apple Music.

We can't have an assessment that has been done on really old technology.

[*Translation*]

Mr. René Villemure: That's a good comparison.

Policies are already in place, and those policies are part of the organization's structure. It seems to me that the structure isn't the problem, because the directives and policies are there. The problem is that they aren't followed.

Do we need more directives and policies, or should we instead focus on the culture that exists? As I listened to the officials, I thought to myself that leadership starts at the top. That isn't happening, so what do we do?

[*English*]

Ms. Jennifer Carr: Again, let's talk about repercussions. You now have 13 departments that said they didn't do them: “Oops, sorry.” There are no repercussions.

It's going to take repercussions. It's going to take you taking away authority from deputy ministers. It's going to take you actually getting into the weeds and saying that since they didn't follow, you're going to roll back their authorities.

● (1240)

[*Translation*]

Mr. René Villemure: Say we take those actions. Do you think it will restore the trust of your 75,000 members?

[*English*]

Ms. Jennifer Carr: If there are actually repercussions for people who don't follow the policies and directives, it will, 100%.

We are really good at making sure that public servants are following the policies. Why are we not putting that same scrutiny on deputy ministers?

[*Translation*]

Mr. René Villemure: All right.

I'm going to ask you the same question, Mr. Prier. Do you think that would help restore people's trust?

[*English*]

Mr. Nathan Prier: I agree completely with Jennifer on this one.

Enforcement measures and serious consequences for breaches of privacy need to be taken seriously. The next steps that need to be taken are entirely at the level of senior management being disciplined for allowing these breaches to occur in the first place.

We talk about a culture change. Culture is a very vague thing to change. I think serious consequences for breaches of privacy are, in fact, the steps we need and we need to get specific on what those are each time this happens.

[*Translation*]

Mr. René Villemure: When deputy ministers are told that they are expected to do X, Y and Z, should we include privacy protection as one of those things?

[*English*]

Ms. Jennifer Carr: Again, every public servant is a Canadian citizen, as you are a Canadian citizen. I think we have to have clear lines on what your privacy is. We should expect a level of privacy. You should not be able to look at my kids' photos just because—

[*Translation*]

Mr. René Villemure: Sorry, I'm going to stop you there.

Ms. Jennifer Carr: Yes, go ahead.

Mr. René Villemure: I'm almost out of time, so I'm going to be quick.

The government communicates its expectations to deputy ministers. Should those expectations include protecting privacy?

Ms. Jennifer Carr: There is no short answer to that.

Mr. René Villemure: I will take that as a yes.

Ms. Jennifer Carr: All right.

Voices: Oh, oh!

Mr. René Villemure: Thank you, Ms. Carr and Mr. Prier.

The Chair: Thank you, Mr. Villemure.

[*English*]

Ms. Carr, you'll be glad to know that Mr. Brock and I still play Pong on our Commodore 64.

Voices: Oh, oh!

Ms. Jennifer Carr: And you still have Napster.

The Chair: No. I have Apple Music. It's $14.95 a month. I know that.

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

Mr. Matthew Green: Thank you very much.

I'm just happy to be able to report that I downloaded the first Wu-Tang album on Napster 20-plus years ago. Now they're doing retirement reunion tours, so here we are.

I want to pick up from where my colleague left off on what I think is a generally accepted notion of informed consent.

Would you agree that your members—understanding the policy directive of the Treasury Board that technology implemented within the federal government must undergo a privacy impact assessment—would have a reasonable expectation that all technologies would have undergone that process, as per the direction of the Treasury Board?

Would that be a reasonable expectation?

Ms. Jennifer Carr: I would disagree, because of the policies that exist, which say you can use it for personal use. They haven't been clarified.

I pose to you, if deputy ministers aren't following their own directives, how are the employees—

Mr. Matthew Green: I want to make sure you understand what I'm asking.

I'm suggesting there's a directive from Treasury Board. We've heard testimony that departments are not following the directive, so would your membership...? Understanding that it is a policy that this should happen, this ought to happen, is it reasonable for departments to assume that it has happened, even though we've heard that it hasn't?

Ms. Jennifer Carr: Yes, if there's a directive.... Treasury Board says all the time that there are directives that need to be followed. I expect that departments should be following those directives. They are the senior leaders.

Mr. Matthew Green: Mr. Prier.

Mr. Nathan Prier: Our members do have that expectation. They feel their trust has been completely breached, because of the violation of a very clear policy on this. They then have an anxiety around using devices to which they have a reasonable expectation of privacy as laid out in policy.

Mr. Matthew Green: Do you think the Office of the Privacy Commissioner should perhaps be reviewing, in a default way, all of these technologies, particularly the ones that could be surreptitiously collecting data?

Mr. Nathan Prier: I do, yes.

Mr. Matthew Green: I bring that up because you talked about removing authority.

Should they have the authority in the first place?

Ms. Jennifer Carr: Whether it lies with the Privacy Commissioner or deputy ministers in their department.... You have seen with the 13 departments that they scrambled to give you information, they scrambled to know where it was being used, and they scrambled to provide you with testimony. There should be clear accountability at the deputy minister level, or it should reside with the Privacy Commissioner.

Mr. Nathan Prier: The Office of the Privacy Commissioner is the proper place to do this. In a lot of cases, and in the case of Treasury Board directives, deputy ministers are left with their own discrepancy and their own decision-making powers, when it's convenient for the employer, and then it's—

● (1245)

Mr. Matthew Green: It's a bit of a Wild West.

Mr. Nathan Prier: Yes, it's a bit of a Wild West in terms of consistency in the application of policies, except when it's convenient for the—

Mr. Matthew Green: Quickly, have there been any grievances?

Ms. Jennifer Carr: We don't know of any grievances, but in order for us to file a grievance, we have to know that the act is taking place.

Mr. Matthew Green: That's correct.

Would a lack of grievance be a permission for them to breach the Privacy Act?

Ms. Jennifer Carr: Absolutely not.

You can't grieve something if you don't know it's happening. The minute you understand that it's happening, you can make your grievance, but if you don't know it's happening, you can't protect your rights.

Mr. Matthew Green: Mr. Prier.

Mr. Nathan Prier: A grievance could be something that could move the needle a little bit on this. We're looking at ways to enforce our members' rights in this case, but the case is that the policies exist and should have enforcement rights built in at that management level.

Mr. Matthew Green: Should we review the Privacy Act?

Ms. Jennifer Carr: Yes, 100%.

Mr. Matthew Green: What would you like to see in it?

Ms. Jennifer Carr: The notes I had for the Privacy Act were that the guidelines had to be clear around what, when, and how new or modified requirements needed new privacy assessments, and when current ones needed to be updated. We also need to make sure it is enforced. These software tools need to be assessed before being used, and all less invasive methods must be considered beforehand.

Mr. Matthew Green: Mr. Prier, do you have anything to add to that?

Mr. Nathan Prier: The employer needs to take its responsibilities to its workers and the Canadian public seriously. The point has been made over and over again about these being Canadian citizens, as well as federal public servants. When digital policies are out of date and not respected, we find ourselves with spyware on government devices, and, clearly, enshrined rights are not respected.

The Privacy Act could be updated in all these ways, but there are strong tools in place right now with no enforcement mechanisms and no consequences for their breach.

Mr. Matthew Green: I want you to have the ability to answer a question that has been kind of generally posed by some of the departments. Tools are being used to look into government policy violations, such as fraud or workplace harassment, so shouldn't the government have the right to look into these serious violations?

Ms. Jennifer Carr: If they are using these tools the way they're supposed to, for what they're intended and under the data privacy assessment that has been done, we need to make sure that.... We heard from three departments. They said they used them without doing the prior assessments. We need to make sure that the assessments are being done as they're intended.

Mr. Matthew Green: Mr. Prier.

Mr. Nathan Prier: I have nothing to add to that.

Mr. Matthew Green: As we contemplate final recommendations, notwithstanding that your membership will likely be tuned into this issue now, what steps can we take to help restore some trust from the general feeling of having something that is now, I would argue, fully integrated into every aspect of life? You referenced the way in which applications on the phone.... I have an iPhone. I have an Apple Watch. I have the biometrics. All the different ways in which.... I have my banking information. Everything is there.

How can we help, in this committee, to restore some of the trust from your membership back towards senior management?

Ms. Jennifer Carr: It all comes back to accountability. If we have the directives, what happens when people don't follow directives when they're asked to do something prior to...?

Again, as I said in my statement, the government needs to acknowledge that we're Canadian citizens as well and that when we're using an employer device, it does not mean that our employer has ownership over all the data that is contained within it.

Mr. Nathan Prier: A full review of digital policies and a mechanism to update them along with new technologies would be ideal.

I want to just raise the point again that as the largest employer in Canada, the federal government has the power—and pretty specific powers—to be able to impose policies that do things like proactive disclosure, informed consent and the enforcement of privacy policies in ways that maybe imposing that on the private sector does not. Therefore, we have a benchmark-setting role here, as one of the largest employers in the country and also as the Government of Canada, to be able to do this with powers that might be muddier when it moves into the private sector. There's a benchmark setting here that matters for all Canadians and our members.

The Chair: Thank you, Mr. Prier.

Mr. Green, it was an important question, so I did give extra time for a response. There was also the fear that Mr. Green would file a grievance against the international association of chairs of committees.

Mr. Brock, you have five minutes.

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

Go ahead, Mr. Brock.

Mr. Larry Brock: Thank you, Chair.

Thank you to the witnesses for their attendance.

Earlier this week, the Auditor General, as you know, released a bombshell report exposing incompetence and corruption within the CBSA. I think the most glaring problem with this report is how the government, despite its promise in 2015 to reduce the use of external consultants and rely upon the professional public service.... We know that, over the years, it has increased the size of the public service by close to 40%.

How do you feel, as union leaders, and how does your membership feel, knowing that GC Strategies—a two-person firm working out of their basement with no IT experience—was simply connecting government with IT professionals? How do you feel about that egregious abuse of the expertise that your membership holds?

● (1250)

Ms. Jennifer Carr: I'm going to take that because I represent the IT workers.

I'll say that we are livid. I would love to come back to this committee. There's lots I could talk about with regard to this whole contracting out.

I had a member come to me this week and say that they can't even get a pencil and a notebook without two people signing off on authority, so how could something balloon so big?

I would love the opportunity to come back. I didn't prepare for that testimony today, but I would love to come back and talk to you about it.

Mr. Larry Brock: You have three and a half minutes. Can you elaborate some more? I'd love to hear more.

Ms. Jennifer Carr: Contracting out has been a preoccupation of the Professional Institute of the Public Service of Canada. We represent professionals, including engineers, nurses and doctors—all regulated professionals who take their work on behalf of Canadians very seriously.

To watch things be contracted out.... It leads to higher costs to the government—it was 40% higher in the report—as well as less transparency, less accountability and lower quality of service. Most important, for me, is the loss of institutional knowledge because it is done out of house. That means we have to consistently be interdependent on contractors to even correct mistakes that they have made.

We need to make sure that we invest in the public service, so that they can maintain and deliver the reliable services on which Canadians depend and which they expect.

Mr. Larry Brock: Thank you very much.

Given the future expansion of our work here at the ethics committee, I'm sure we're going to see you again, Ms. Carr. Thank you for that.

I'll go over to Mr. Prier and Ms. Shantz with the same type of question.

Do you have any thoughts on that?

Mr. Nathan Prier: This was an egregious violation of procurement policies and an egregious violation of...a lot of different ways in which contracting out has bloated what people generally read as the public sector. Public servants actually do not make up the entirety of the public sector. A huge amount of that is shady relationships and contractors—which are sometimes needed, of course.

I'm speaking here as a policy analyst and as the president of a union that represents a lot of policy analysts. Even in that specialized world of policy development, contracting out is normal. There are databases we don't have access to. There are fields of information that we just can't have access to, but this whole element of not being able to build the institutional memory to be able to carry out our tasks in a regular way is a consistent problem.

When people talk about the bloat of the public sector, for our members it's these vast webs of contractor relationships that could probably be done far more cheaply, more effectively and in the spirit of building institutional memory and capacity in-house.

We do not believe that the public sector is overly bloated. We don't agree that the public sector requires a lot of trimming over the next five to 10 years. We do need this contractor relationship and this vast web of contractors to be severely reined in, however, because we feel that our members are qualified to do the type of work we do best, with the correct levels of oversight, which are very stringent levels of oversight.

Mr. Larry Brock: Thank you.

Ms. Shantz, what are your thoughts?

Ms. Laura Shantz (Senior Advisor, Advocacy and Campaigns, Canadian Association of Professional Employees): I would just like to add this briefly. We're here today to talk about privacy. The minute we start adding layers of contracting out, all of a sudden we have infinite points for data breaches. We saw it with BGRS moving. Recently there was another one; I can't remember the name right now.

We see these things start to happen. All of a sudden, when we start contracting more and more, we open ourselves to more and more points of failure and more and more points of breach. That needs to be thought about in a holistic way, how we can maximize security, because that's Canadians' personal data, public sector workers' personal data and data that is important to our government from security perspectives.

This is essential stuff. It's stuff that public sector workers are trained on. They know how to do it and how to get it right. When we contract that out, we start losing control. That's something we need to be thinking about as well.

Mr. Larry Brock: Thank you very much, all of you.

The Chair: Thank you, Mr. Brock.

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

● (1255)

Mr. Francesco Sorbara (Vaughan—Woodbridge, Lib.): Thank you, Mr. Chair.

It's great to be here with you as chair and with all my honourable colleagues. It's been two or three years since I've sat on the ethics committee. I sat here for a period of time. I always find this committee to be very important in many ways. It undertakes a lot of serious studies, I would say.

I welcome the panel members here today.

First off, I want to say to the panel members, to all your members and to all the employees of the federal public service, thank you for everything you do, not only for what the members of the Library of Parliament do to help us MPs out, but also for what you do for literally millions and millions of Canadians every day in delivering services and benefits to them.

I would also like to say that we have hired folks in the federal public service over the last several years. We have rebuilt it after the devastating cuts, as I would characterize them, from the prior administration, from the Harper government. They literally cut to the bone. We know what it was like to be a federal public servant under a Conservative administration, do we not?

First off, the member for Brantford—Brant recently said here at committee that if people are public servants, there are no privacy issues.

I'll ask you, Jennifer, and you, Nathan, do you believe public servants are entitled to privacy?

Ms. Jennifer Carr: They are entitled to their privacy, 100%. Again, we are Canadian citizens. We do not pledge allegiance to one government. We have autonomy. We can be political. We should not be able to lose our privacy rights just because we work for the federal government.

Mr. Francesco Sorbara: What about you, Nathan?

Mr. Nathan Prier: I believe that as a point of principle. I believe that's been established in policy, as Jennifer has alluded to a number of times here.

Mr. Francesco Sorbara: Okay.

With respect to privacy, I have the pleasure and honour of sitting on the industry committee. With Bill C-27, there's an aspect of privacy in that, with PIPEDA and the relevant sections and so forth. Privacy is a huge thing these days, which is an understatement—I'm using very common language, if I can say that—in terms of striking a balance. Like many of our representatives, I worked in the private sector before I had the distinct pleasure of serving the residents I currently serve. When you are provided a device from your employer to utilize, it is their device. You need to use it with judiciousness and diligence. There's a balance there. I've always seen that a balance needs to be struck.

Within that, within the government operations, there have to be guardrails within the departments, and they need to follow the PIAs, the privacy impact assessments. I literally learned this in the last couple of hours. I sit on two other committees, so it's been a busy week. With the PIAs, there is an agreement that when investigations need to happen, they should happen, and the devices and the contents of those devices need to be looked at.

Also, taking a step back, if I'm working for Nathan's organization and I enter into an agreement with the federal government, there is consent that you will use this device but you will use it responsibly. I'm putting that out there, because there needs to be that balance. If processes were not followed properly, you would need to correct those internal processes and the governance, of course.

Do you not agree that consent is important and that balance is important, but the notion that there has to be responsibility on the end-user is important as well?

Ms. Jennifer Carr: Yes. It's a shared responsibility. But if you don't tell me up front what I can and cannot do, if you do not disclose that you are going to go in.... If I access a website to get at my photos, you can then delve through those spiderwebs and touch everything I've used. That has not happened at this point.

Mr. Nathan Prier: I believe those boundaries are being established, and the right to the privacy of your personal use of the phone or of the other device has also been kind of established. We're finding the different guardrails as we go here.

I would say that's not what we're talking about here right now. We're talking about the proactive disclosure of a technology that should have been disclosed to those employees using those devices. When we're talking about informed consent, we believe it goes way past informed consent when we have to find out what technologies are on our devices through an access to information request and not through that proactive disclosure.

Mr. Francesco Sorbara: How much time do I have, Chair?

The Chair: You have 35 seconds.

Mr. Francesco Sorbara: At this time, I just want to get a clarification. Currently, when someone is hired and joins the federal public service, and has gone through the rigours and processes, what consent or information is provided to that individual?

I'll hear from Jennifer and then Nathan, quickly.

Ms. Jennifer Carr: It is a mix, depending on the department you work for. Obviously, I believe you are provided with your values and ethics. That's the requirement, and you have to sign off on that. Other than that, I don't think there is a set package for every department.

Again, as we decentralize and allow departments to take over the individual policies, it depends.

● (1300)

Mr. Nathan Prier: I've worked for multiple departments and can tell you that it's wildly inconsistent in terms of how a new employee or somebody who's getting a new device is trained and given the ability to consent to what they're consenting to.

Yes, it is a shared responsibility, of course, but in some cases, it has felt more like the terms and conditions of a new iPhone when I'm being told about the various rights and responsibilities I have with a government device. Training might be something that's necessary, but again, I don't think that's exactly what we're talking about here.

The Chair: Thank you.

Thank you, Mr. Sorbara.

[*Translation*]

It is now over to Mr. Villemure for two and a half minutes.

Mr. René Villemure: We've talked about the code of values and ethics for the public service, but let me tell you that it doesn't provide much in the way of clarity.

I'm going to follow up on a question I asked in the last round.

In the past, deputy ministers were told that they had to meet certain expectations in relation to the code. Their knowledge of the code and their ability to implement it were assessed. I'm not sure how successful that was.

Ms. Carr, do you think similar expectations as regards privacy should factor into a deputy minister's performance assessment? In other words, come the end of the year, practices they had introduced or their compliance with privacy measures would be assessed.

[*English*]

Ms. Jennifer Carr: That's a big question. We're talking about performance management. I have lots of things to say on that as well.

Yes, if you had a checklist of policies that you say they didn't comply with, then it is important to find out how many people filled out their ethics survey and that sort of stuff.

I think it's a bigger question—

[*Translation*]

Mr. René Villemure: Sorry to interrupt you, Ms. Carr, but I don't have much time.

Do you want to answer that, Mr. Prier?

[*English*]

Mr. Nathan Prier: I believe performance management might be one way to do this.

I think consequences for privacy breaches should be the true tool we're using here.

[*Translation*]

Mr. René Villemure: One of the things we were told a lot is that using the tool was the only way to achieve the desired outcome. Do you think that's true?

[*English*]

Mr. Nathan Prier: Do you mean whether the access to information request was the only way to get—

[*Translation*]

Mr. René Villemure: I'm talking about deploying the tool on devices.

A lack of supervision tends to lead to certain behaviours. Better supervision would prevent certain behaviours and thus obviate the need for surveillance.

[*English*]

Ms. Jennifer Carr: I think that's the whole point of the privacy impact assessment. What information are you trying to get? Let's talk about the time theft. Let's talk about whether people are at the workplace. Can we obtain that information through other means, other than going invasively through a device?

That would be why the assessment exists, and it should be the primary focus of getting the data in a less intrusive manner.

[*Translation*]

Mr. René Villemure: That's great.

[*English*]

Mr. Nathan Prier: I don't have much to add to that, except that the proactive disclosure element of a new technology being used is really at the core of where the trust was breached here. Keeping that in mind, regardless of the results of what the technology was trying to achieve, as much as that's a bigger conversation, I think the proactive disclosure element here, just to add to what Jennifer said—

[*Translation*]

Mr. René Villemure: Thank you.

The Chair: Thank you, Mr. Villemure.

[*English*]

It's over to Mr. Green for two and a half minutes.

Mr. Matthew Green: Thank you very much.

Often, in preparing for these committees, you go through a set of questions that might be asked and review really important points you want to make. Sometimes, we fail to ask those questions.

Are there any points of interest or answers you'd like to provide this committee beyond your opening statement and beyond the questions that have been asked?

Ms. Jennifer Carr: I will actually be at the defence committee in two weeks, talking about contracting out.

The overall accountability and the decentralization of responsibilities to departments has created an environment where it's hard for me to tell my members what rights they have, how they're going to be applied and what policies are going to refer to them, and provide them guidance.

I would really like to say we all work for the federal government and we have one employer. However, we have many different rules and regulations, depending on where we work.

Mr. Nathan Prier: I believe most of my points were made today.

Thank you.

Mr. Matthew Green: Should you have any additional points, or should you hear information you'd wish to have a rebuttal to, notwithstanding the next session with the Treasury Board, please feel free to submit that to the committee for our consideration.

We really appreciate your work.

Ms. Jennifer Carr: I'll definitely get you that directive so that every committee member knows that it is allowed.

Mr. Matthew Green: I'll also put on the record, in my remaining time, that I'm not shocked that union reps came with solutions. I know that the former president of a firefighter association, our chair, is also not shocked.

Thank you for being here today. I appreciate your testimony.

● (1305)

The Chair: Thank you, Mr. Green.

That concludes our panel for today.

I want to thank all of you for being here in front of committee on this important study. I also want you to relay a message on behalf of the committee to your members to tell them how much we appreciate the work they do on behalf of Canadians.

Without any further business, that concludes today's meeting.

I want to wish everyone a good week in their constituencies.

We're going to be back here on the 27th with the RCMP commissioner in relation to SNC-Lavalin.

Thank you to the clerk, the analysts and the technicians for all their help in putting this meeting together.

The meeting is adjourned.