HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

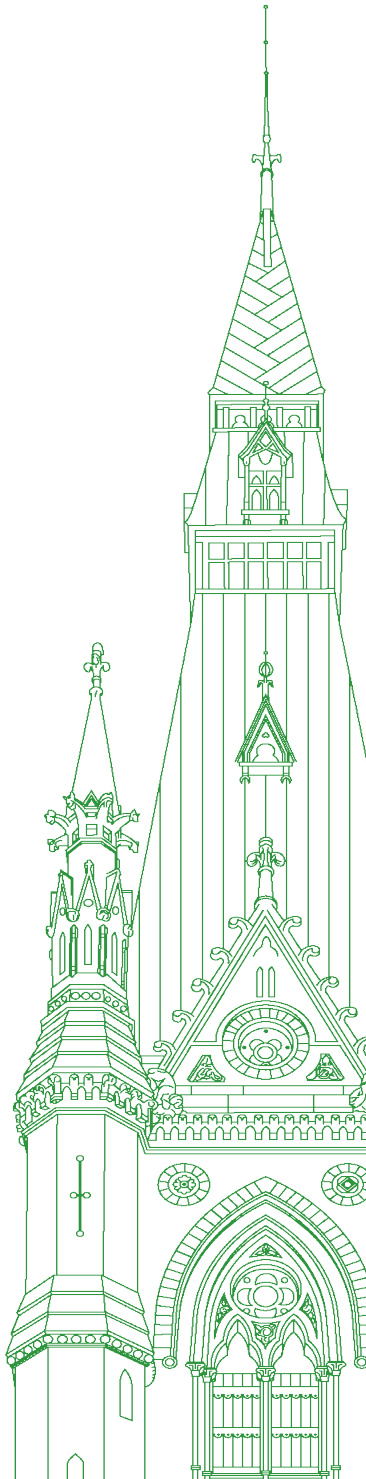
44th PARLIAMENT, 1st SESSION

Standing Committee on National Defence

EVIDENCE

NUMBER 101

Wednesday, May 1, 2024



Chair: The Honourable John McKay

Standing Committee on National Defence

Wednesday, May 1, 2024

● (1710)

[*English*]

The Chair (Hon. John McKay (Scarborough—Guildwood, Lib.)): I call this meeting to order.

As you can see, we're under some time constraints, so I'll be seeking unanimous consent to go when the bells ring. That's number one.

Number two is that I would like to get the report of the subcommittee adopted, and I would like to get the budget adopted.

I would also like to get some indication from those of you who are here as to whether you will be here for the meeting with the German defence minister on Friday, May 10.

That's my wish list. How far along I'll get with my wish list, I don't really know.

I feel constrained to read the regulations with respect to these earpieces. They are new, but they're still important.

To prevent disruptive and potentially harmful audio feedback incidents, all earpieces have been replaced by a model that reduces the probability of audio feedback. All unused earpieces will be unplugged at the start of a meeting. If you are not using your earpiece, please put it face down in the middle of the sticker for this purpose. Please consult the cards for guidelines.

The room has been adjusted, as you can see. There is a lot of space. I can barely see our witnesses' names, but this is the new reality.

With that, I'm going to invite Mr. Dufresne to speak on behalf of the Office of the Privacy Commissioner of Canada.

You're very familiar with this committee and all committees on the Hill. I want to take note that over the years you've been very generous with me, and I appreciate that courtesy and that competence.

Sir, you have five minutes.

Mr. Philippe Dufresne (Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada): Thank you, Mr. Chair and members of the committee, for this invitation to appear as part of your study of transparency within the Department of National Defence and the Canadian Armed Forces.

I'm accompanied by Isabelle Gervais, deputy commissioner of compliance, from my office.

As this is the first time I have appeared before this committee, let me begin by discussing my role as the Privacy Commissioner of Canada and the role of my office, which we refer to as the OPC.

As Privacy Commissioner, my mission is to protect and promote individuals' fundamental right to privacy. This includes overseeing compliance with both the Privacy Act, which applies to federal institutions' collection, use, disclosure, retention or disposal of personal information, and the Personal Information Protection and Electronic Documents Act, or PIPEDA, which is Canada's federal private sector privacy law.

[*Translation*]

As an agent of Parliament, I report directly to Parliament. Through written submissions and appearances such as this one, I provide analysis and expertize to help inform Parliament’s review of evolving legislation and recommendations on privacy issues.

The Privacy Act defines personal information as any recorded information about an identifiable individual, including a person’s national or ethnic origin, colour, religion, age, marital status, as well as medical, criminal or employment history, and social insurance number.

The Privacy Act provides individuals with the right to access the personal information that the government holds about them, and to request corrections to that information where necessary.

[*English*]

My office investigates complaints that are made against federal institutions under section 29 of the Privacy Act, which includes cases when individuals have been refused access to their personal information or instances when the institution is taking too long to respond to a request.

My office also investigates issues relating to the protection of personal information, such as allegations of improper collection, use, disclosure, retention or disposal of personal information. This includes matters involving privacy breaches.

While I am responsible for oversight of the Privacy Act, my colleague Caroline Maynard, the Information Commissioner of Canada, who has also appeared before you on this study, administers and enforces the Access to Information Act. The two pieces of legislation were enacted together in 1983 and are intended to be a "seamless code" of informational rights that carefully balance privacy and access.

The Privacy Act has not been significantly updated since it was passed 40 years ago. The justice department published a consultation paper in 2021 and is still consulting on Privacy Act reform. One of the issues it discusses is the government's approach to transparency.

I support the enhancements to transparency that are proposed in the paper, and my office has made recommendations for future improvements. Transparency is important in empowering citizens with the knowledge they need to exercise their rights and in requiring the government to be accountable for its handling of personal information. These are critical aspects of a meaningful data protection framework.

● (1715)

[*Translation*]

With respect to this committee's study being discussed today, my office has had ongoing engagements with the Department of National Defence. In the past five years, the department has consulted the OPC on a wide range of privacy-related issues such as biometrics, open-source intelligence, staffing and recruitment.

My office has worked with the department and Canadian Armed Forces to provide advice on compliance with the Privacy Act.

My office has accepted nearly 300 privacy complaints against the Department of National Defence and the Canadian Armed Forces over the last five years. More than half of these were related to the time that it was taking them to process requests for access to personal information.

[*English*]

In the same five-year period, the OPC received 10 breach reports from the organization, which were primarily related to unauthorized access, unauthorized disclosure and the loss of personal information.

I welcome the efforts the Department of National Defence and the Canadian Armed Forces have made towards privacy protection, and my office remains available to provide support and advice. I encourage them to prioritize timely responses to requests for access to personal information and also to undertake privacy impact assessments before onboarding new programs and processes.

With that, I will be happy to answer your questions.

The Chair: Thank you, Mr. Dufresne.

We'll start with Mr. Kelly.

Colleagues, if there's any chance of getting into a second round, I'm going to have to cut back the first round. We're going to go with four minutes for the first round, and then we'll go from there and see how far we can get.

Thank you.

Mr. Kelly, you have four minutes.

Mr. Pat Kelly (Calgary Rocky Ridge, CPC): What do you consider an acceptable time frame for a privacy request related to a sexual misconduct case?

Mr. Philippe Dufresne: It's all context-based. The legislation talks about a 30-day period for a response, and then there is the possibility of an extension for another 30 days. We would look at those cases on a case-by-case basis.

Mr. Pat Kelly: Okay. On April 17, we had a witness who told this committee that "complaining to the Information Commissioner and the Privacy Commissioner is not an exception to getting the information. It is part of the process. You will not get your information unless you make a complaint."

It was put to the committee that delay is commonplace, and the department will delay and force the applicant to complain.

Do you have any comment on that?

Mr. Philippe Dufresne: As I've indicated, I think the bulk of the complaints we receive deal with delays to the process in terms of personal requests.

Mr. Pat Kelly: Is it a failure of leadership to ensure that openness and proper disclosure are actually done?

Mr. Philippe Dufresne: What we see is that there are many cases in which the delays are greater. We work with the departments. We deal with the complaints. We've found that departments are collaborative in the complaints process as they work with us, but that is an important part of the number of complaints and volume of complaints we receive. We try to resolve them as early as possible through resolution and expedited complaints mechanisms.

Mr. Pat Kelly: The Information Commissioner, in her report, mentioned that "senior leadership is key to influencing corporate culture change" to actual compliance and timeliness under her act. We're now two defence ministers later—this was a 2020 report—and we hear the same complaints of slow service, intentional avoidance and the culture of secrecy that appear to apply to requests under both the Privacy Act and the Access to Information Act.

Do you agree that ministers must, and this is in her words, "see it as their responsibility to champion a new approach, and to adopt these tools and practices in order to effect the necessary changes within the department".

● (1720)

Mr. Philippe Dufresne: I agree that leadership is important, and I agree that access to information and privacy are fundamentally important legislation, so they should be prioritized.

Mr. Pat Kelly: Okay. We also heard from the same witness, Patrick White, on April 17, that "a significant barrier and challenge I'll highlight is that you are required to name the individual record holder in trying to get access to your personal information."

He equated this to the equivalent of trying to get a tax assessment of your own from the CRA and being required to have the employee ID number of the actual employee who may have handled it.

Do you have a concern around privacy and the level of information the applicant for information needs to get information about themselves?

Mr. Philippe Dufresne: I think the department should make efforts to make the system as user friendly as possible. One of the themes I've been pushing in terms of privacy in all aspects is really making sure we are not delegating to individuals and to citizens.

Mr. Pat Kelly: Is the system now user friendly?

Mr. Philippe Dufresne: I think what we're seeing in the system is lengthy periods of time, so that's something that....

Mr. Pat Kelly: We're seeing lengthy periods of time for delays.

The Chair: Thank you, Mr. Kelly.

Mr. Collins, please go ahead for four minutes.

Mr. Chad Collins (Hamilton East—Stoney Creek, Lib.): Thanks, Mr. Chairman.

Welcome to our witnesses.

In a perfect world, we'd have perfect compliance with the legislation and the acts as they exist. Of course, the world isn't perfect, so we have people who are in non-compliance situations.

Can I ask about the education and outreach services your office provides to those in CAF or elsewhere to ensure people are properly trained? Also, when someone is making their way through the system, how do you know they're actually following the rules?

Mr. Philippe Dufresne: That work really is done by my office and by the Treasury Board Secretariat. The Treasury Board Secretariat will be providing guidance and information to the departments themselves. In terms of best practices and expectations, one example of that is the directive on privacy impact assessment, which I hope will be made a legal requirement. Right now, it's something that is in Treasury Board policy, but it's not in law. They play very much that education role with the departments. We work with Treasury Board and we are consulted by Treasury Board, and we would want that to continue and increase so our perspective informs the Treasury Board directives and the training Treasury Board will do.

We have government advisory services within my office that are available to assist and provide input to departments for new programs and initiatives and to be consulted on privacy impact assessments. Certainly, we are doing that in tandem with the Treasury Board Secretariat.

Mr. Chad Collins: The committee has received a lot of recommendations in terms of constructive criticism as it relates to improving the system and how it operates. You must deal with your provincial counterparts. Is there anything to learn from their acts, which, in many instances, have been updated and are not 40 years old? Can you provide to the committee recommendations in terms of what we can learn from some of those other jurisdictions within Canada that have made improvements?

Mr. Philippe Dufresne: One of the improvements, certainly, that I would like to see in the privacy legislation, for both the public and private sectors, is order-making power. That is something Parliament has given now to the Information Commissioner in terms of access requests, which was a positive step in Bill C-58. It is something that is currently proposed in Bill C-27 for private sector privacy legislation, and I would want this to be part of public sector privacy legislation. That was one of the recommendations in the Justice Canada paper.

Specifically with respect to access matters, I would want this to be expanded to all matters. I think this is an area in which some of our provincial counterparts and, indeed, our international counterparts are ahead, with the authorities to make not merely recommendations but also orders. That's one area.

I would be remiss if I didn't highlight the very strong collaboration I have with my federal, provincial and territorial counterparts in this space. That collaboration has led to joint investigations and joint statements and resolutions, so we're going to continue to work very closely with them.

Mr. Chad Collins: You talked about privacy impact assessments at the end of your statement, but you didn't elaborate on those. Can you highlight what they are and their importance?

Mr. Philippe Dufresne: A privacy impact assessment is really a due diligence tool whereby the organization thinking of putting in place a new program or tool that can have privacy impacts is required to assess the impacts and look at the risks and document them, and think of solutions to mitigate those risks, in consultation with my office. It's a very powerful tool that is a good practice and is good for everybody. It's good for citizens, who are going to have better privacy protections, and it's good for the departments, because they get advice and are seen to be getting advice from a neutral regulator. This is absolutely something that should be done in all cases and before new tools and new programs happen. In reality, that doesn't always happen, which is why it should be a legal requirement, in my view.

● (1725)

The Chair: Thank you, Mr. Collins.

[*Translation*]

We now go to Ms. Normandin for four minutes.

Ms. Christine Normandin (Saint-Jean, BQ): Thank you very much.

Mr. Dufresne and Ms. Gervais, thank you for coming.

Mr. Dufresne, in light of a question I've put to other witnesses in a previous meeting, I understand from some members of the forces that when information is added to their file and someone accesses it, there is no way to track who consulted that file. Is that something that has ever been brought to your attention?

Mr. Philippe Dufresne: That example doesn't bring anything to mind.

Ms. Christine Normandin: If that scenario were accurate, could it cause problems that might fall under your jurisdiction or under the Privacy Act?

I'm drawing a parallel with what happened to Véronique Cloutier, who found out that 400 individuals had needlessly accessed her medical file.

It seems that military personnel don't know who or how many individuals have accessed their file. For example, it might be someone who is the subject of a complaint made by that military member. If that's the case, what problems could arise?

Mr. Philippe Dufresne: One of the problems that could arise concerns the reason the individual obtained the information: It needs to be a legitimate reason and relate to the organization's legislative mandate.

Second, the information collected must be protected. It must not be disclosed without cause and any disclosure of the information generally needs to be related to the initial reason it was collected.

When information is provided, not everyone in government needs to know it. If information is shared for purposes other than its intended purpose or if it isn't adequately protected, that's where privacy breaches can occur.

Ms. Christine Normandin: Thank you very much.

On another subject, I'd like to hear your comments on artificial intelligence, or AI. I understand that you've done studies on ChatGPT, among others. As a result, you know how user data is being used, retained and shared.

The Minister of National Defence said that the army is likely to make increasing use of AI in the future. This is also true of the United States, which signed agreements with Amazon and Google.

Could you comment on the risks associated with the armed forces' use of AI on the personal data of military personnel and others?

Mr. Philippe Dufresne: Indeed, an investigation into ChatGPT, which I am conducting jointly with my counterparts in Quebec, British Columbia and Alberta, is still ongoing.

My G7 colleagues and I hold frequent discussions, both at the ministerial level as well as among fellow privacy commissioners. We released a statement on AI in which we stressed not only the need to adopt new laws and modernize others, but also the fact that existing legislation, including privacy laws, is already applicable to AI.

In December, my provincial and territorial counterparts and I released a statement in which we put forward various privacy principles that we want to see implemented. It refers in particular to consent, lawful authority, rigour, security and the consequences of using AI, including—even if it's not exactly within our mandate—the issue of discrimination.

The advantages of using AI need to be identified, because there are many, but guidelines also need to be established, even with existing legislation.

Additionally, with my colleagues from the Canadian Radio-television and Telecommunications Commission and the Competition Bureau, we created the Canadian Digital Regulators Forum to cooperate on these issues, particularly ones involving artificial intelligence. The considerations go beyond privacy, competition and discrimination, so we need to work closely together, even on national security issues.

That's certainly an important file for us, and one of my office's strategic priorities.

● (1730)

The Chair: Thank you, Ms. Normandin.

[*English*]

You have four minutes, Ms. Mathyssen.

Ms. Lindsay Mathyssen (London—Fanshawe, NDP): Thank you for joining us today.

Earlier in this study, we heard from Michel Drapeau that when CAF members are filing grievances and cannot access their information, your team is in place, and that's the only way they can access some of that. You mentioned before that so many of the cases you deal with are lagging behind in terms of being able to get information. Even with the investigations that your office can take on, they take about a year or so, which creates a lot more delay in terms of that pursuit for information on their grievance.

Can you tell us where the delays are created and what's being done, if anything, by DND-CAF to improve that?

Mr. Philippe Dufresne: I can tell you certainly that, throughout, we are seeing this issue of delay as being an important one to tackle—for ourselves as well, the complaints, the process that we have. We've put forward as one of our strategic priorities the notion of looking at our own processes and whether we can make those more efficient. We've obtained resources from government and Parliament in terms of dealing with backlogged cases, prioritizing certain cases, and looking at our processes to see if they're as efficient as they can be and whether there are things that need to be changed.

That should be done by departments as well. That's where putting it as a priority, making sure that you are challenging your processes, you're removing inefficiencies and you're making sure that these things can proceed efficiently is certainly very important.

Ms. Lindsay Mathyssen: The deputy minister of defence said that the department was doing that.

In your opinion, is that the case?

Mr. Philippe Dufresne: I can speak about my office. We are still seeing some complaints...with time limit complaints. That's a big proportion of that.

I would encourage DND and all departments to continue their efforts in that.

Ms. Lindsay Mathyssen: I have a bill, Bill C-362, that creates an independent civilian oversight agency within the ombudsman's office for CAF and DND. Many witnesses have supported this. Former ombudsmen have supported this.

The reason for that is the need for investigative bodies to have more teeth. As you mentioned before, certainly this could be very helpful.

The department refuses sometimes to disclose information, whether it's to CAF members going through the grievance process, veterans, journalists or researchers. As Mr. Kelly mentioned, the department will only disclose this information.... It's only when your office gets involved that they can get anything.

Can you talk about the teeth, I guess, that your team has on the investigative powers piece? Do you believe that more is necessary for the independence in that role within the offices?

Mr. Philippe Dufresne: Absolutely. We are working with departments on the complaints side, the guidance side and the promotion side. There is good collaboration, but the reality is that we do need to have order-making powers and binding authorities. It just assists.

It's not because I want to issue those orders. The mere existence of that possibility tends to focus the minds of decision-makers. It helps to prioritize efforts in those aspects. This is why it's very important that my office be given these order-making powers in both the private sector and the public sector context.

Ms. Lindsay Mathyssen: Ultimately, when you do find that there's a breach, what happens?

Mr. Philippe Dufresne: We'll investigate it. We'll make a finding. We'll make recommendations. In many cases, but not all, the recommendations are followed, and that's a good thing. That's where the order-making power comes in.

In the case of privacy impact assessment, it's required in Treasury Board policy. It's there. It has to be done before the program is launched. We have to be informed. We have to be consulted. It doesn't always happen. Sometimes it will happen after the program has been launched, which creates more risk for everyone.

The Chair: Thank you, Ms. Mathyssen.

If the clerk's and my math is correct, we can still get another four-minute round in. If we don't, it's the clerk's fault. If we do, it's still the clerk's fault.

With that, Mr. Allison, go ahead for four minutes, please.

Mr. Dean Allison (Niagara West, CPC): Thanks, Chair.

Thanks to our guests for being here today.

My question is, how would you rate the job that DND and CAF are doing based on the fact that we have over 300 complaints...the number of days delayed, etc.?

How would you describe DND and CAF? Would you describe them as being transparent and a good example of a compliant department?

● (1735)

Mr. Philippe Dufresne: We have statistics in our annual report in terms of the number of complaints that we received versus the department. They are certainly among the higher ones, with a higher number of complaints. We have received good collaboration from them. We're working with them to resolve these cases.

On the list, they would be fifth from the top in terms of the number of complaints that we've received.

Mr. Dean Allison: It's in the top 10. Okay, there we go.

What about individuals who get an ATIP sent back that's deemed refused? What are their options?

If it's deemed refused, how do they respond?

Mr. Philippe Dufresne: Their option is to go to federal court. The legislation provides that at that stage, individuals can exercise those rights.

This is the import of that determination. It opens up that recourse with the federal court.

Mr. Dean Allison: It almost seems impossible for an individual to be able to go to court to do that.

Is that correct?

Mr. Philippe Dufresne: Well, it's something they have to do. The onus is on them to do that.

Mr. Dean Allison: Is the only option to go to court and incur some sort of costly legal battle to do that?

Mr. Philippe Dufresne: That's the only option to have enforcement.

That's why having order-making powers to be able to have a decision that will be binding is something we've been recommending.

Mr. Dean Allison: Does the Privacy Commissioner have the same legal authority, when it comes to taking DND to court, as the Information Commissioner?

What types of powers would you have in terms of being able to deal with that?

Mr. Philippe Dufresne: We have important powers in terms of the ability to obtain information from the departments as part of our investigations, so we can do that, but the power that we lack is the power to issue a binding order at the end of the investigation when we make a finding. If we make a finding that the legislation was not complied with, we make a recommendation rather than an order, so that's the critical difference.

There are also some who argue for there to be financial consequences—fines and so on—and that's something that's being proposed in the private sector legislation that's currently being debated in committee.

However, for the public sector, at a minimum, having this order-making power would, in my view, make the process more expeditious, because you would have the investigation by my office, by the regulator, and then you get a decision, and then that decision is binding. Instead of having the individual have to go to court and take those steps, that order applies, and then it would be up to the department to challenge that order in a court process.

Mr. Dean Allison: Do you think it's reasonable for a requester, whether they be a junior member or a vulnerable person, to be able to actually name specific record holders? When the challenges go in, they need to know who has touched the file. How on earth would they ever be able to do that? Would it be an easier process for them to be able to get that information?

Mr. Philippe Dufresne: I don't have a specific area on this, other than to say that the process should be adapted to the circumstance and should be as user-friendly as possible. If you make a process and it's very challenging, or there are disincentives for individuals to use it, that's a concern. The processes should be looked at—there may be specific realities and specific departments—but the idea is to make this process easy to understand and easy to use, so those rights can be exercised.

The Chair: Thank you, Mr. Allison.

In anticipation that the bells are going to start ringing shortly, do I have unanimous consent to proceed for 15 minutes after the bells?

Some hon. members: Agreed.

The Chair: Okay, thank you.

Mr. Fillmore, you have four minutes, please.

Mr. Andy Fillmore (Halifax, Lib.): Thank you very much, Chair.

Thank you, Mr. Dufresne and Ms. Gervais, for your work and for your time and presence here today.

I want to begin by speaking with you about modernization and digitization. I'd like to just briefly at the beginning explore a question that I've asked some other witnesses on this study. Sometimes we can fool ourselves into thinking that going entirely digital and relying entirely on computing to streamline, simplify and expedite processes is the way to go. In the case of your work, would you say that's true? Is it necessary to become entirely digital?

● (1740)

Mr. Philippe Dufresne: In the case of our work, we're looking at a range. It's not entirely digital; we're doing a combination of both. We've designed and created a digital tool, for instance, for a breach, to assess whether a given privacy breach is a real risk of harm, and that's going to give an opinion on that and assist in that. There's a combination of that, but then you're going to have the assessment by the investigator, and you're going to have those decisions, so I think we always have to have that in mind. Digital tools and technology bring significant advantages. We need to harness those advantages, and we also need to manage them so there aren't implications that could harm privacy or other aspects.

Mr. Andy Fillmore: Okay, thank you.

I think you began to answer my second question. What initiatives do you have under way now to modernize and digitize your work within the commission?

Mr. Philippe Dufresne: We've moved forward in terms of information on the cloud, for instance, at the OPC. We are looking at technologies generally to see which ones could be used and how to use them. In terms of our strategic priority, we talked about staying ahead of technology in terms of legal compliance. What that means is that we have a role as a regulator to provide guidance and make decisions in terms of complaints on new technologies, including artificial intelligence.

However, also as an institution, we have a responsibility to be as efficient as possible. If there's technology that can help us do that work better, we have to consider that, but we have to consider that in a way that is protective of privacy, that can serve as an example that says if you're going to use this technology, here's the type of due diligence that you need to do before you use it. One of the messages we've been giving to government departments is that before they use new tools from a private sector organization, they should make sure they do that due diligence, that they have the privacy impact assessment and that they're satisfied that this technology is protective of the privacy of Canadians.

Mr. Andy Fillmore: This is interesting. You really do walk a line in your office. On one hand, you are compelled to be open and transparent, and you're very much about providing information in a free and open way, but, at the same time, you need to protect privacy and protect the people who deserve and need to be protected.

You mentioned a moment ago that you developed a digital tool that helps to de-risk that, and I think we already heard someone mention AI. Are you using AI in cases like that, the tool you mentioned?

Mr. Philippe Dufresne: The tool we've developed is a tool where you will input the types of informational elements about the breach—what happened and in what context and so on—and then that tool will generate a score that will indicate that this looks like it's serious enough, that this looks like a breach you should be reporting. It's designed to help, but it doesn't replace the expertise and the human decision-making. It's an example of using technology for something that can help privacy.

Other examples of privacy enhancement technology would be synthetic data or other types of information where you can use technology to protect privacy. You can achieve the same benefits of data without being able to identify individuals.

We're looking at all of these fears, but, as you indicate, we have to make sure that, whatever we're using, we're doing it in a privacy-protected way.

The Chair: Thank you, Mr. Fillmore.

Mr. Andy Fillmore: Thank you.

The Chair: You have a very tight two minutes, Ms. Normandin.

[*Translation*]

Ms. Christine Normandin: Thank you, Mr. Chair.

Mr. Dufresne, I'd like to continue on the issue of privacy impact assessments, which we've just been discussing.

I imagine you're familiar with the Cellebrite company. I understand that its tools are being used by the Canadian Security Intelligence Service and the Department of National Defence, among others. However, I also understand that, even in the context of a judicial authorization or an internal investigation, the government still has an obligation to carry out a privacy impact assessment. If the government fails to do so, it's in violation of its own law.

I'd like to know what we can do about that. What sanctions can be imposed, or what should be changed to prevent that kind of situation from occurring?

Mr. Philippe Dufresne: In fact, the government is not violating its own law, because conducting such an assessment is not a legal obligation, but currently stems from a Treasury Board directive. Hence, a department that doesn't comply is violating a government directive, not a law. That's the problem we've identified. In our view, there should be a provision in the law that says that when a department develops a new program or uses new tools that may have significant consequences for privacy, it must carry out a privacy impact assessment.

We'll continue to encourage the departments to conduct those assessments, and we'll continue to advocate for legislation making them mandatory. In an ideal world, when the question is asked, the response would always be, “Yes, we carried out an assessment.” The media and parliamentary committees are doing important work by raising those issues.

The idea is not to ban those tools outright. Indeed, police forces must have the tools they need to do their jobs, but they need to be disciplined in their use of those tools, after conducting a privacy impact assessment.

We issued a decision on certain tools used by the Royal Canadian Mounted Police to fight crime. Of course, fighting crime is important and the RCMP has to be able to do so successfully, but we determined that the approach taken to protect privacy was insufficient. Therefore, we'll continue to do this work, but I think that there would be greater compliance if the obligation were enshrined in law.

● (1745)

[*English*]

The Chair: Thank you, Ms. Normandin.

Ms. Mathyssen, you also have a tight two minutes.

Ms. Lindsay Mathyssen: In the previous meeting, we heard from witnesses about the still unresolved Afghan detainees case. The government had prorogued Parliament before the public had a chance to learn the full truth of whether the government was knowingly transferring Afghan detainees, and we wouldn't have known that without specific whistle-blowers and the protection of those whistle-blowers.

Richard Colvin was the diplomat who brought the allegations forward, and we heard that, of course, senior military leadership and government elected officials were involved. They tried to discredit him. There's a lot that was done against that whistle-blower, and there weren't protections in place to ensure that he was protected at that time.

I want to know if you believe that there have been enough legislative changes to effectively protect whistle-blowers, because we certainly heard in this committee as well that, through the chain of command, if things are brought forward, there is often punishment for that.

Can you talk about that in terms of what you've seen and your experience as the commissioner?

Mr. Philippe Dufresne: I think that it's important that people be able to access legal recourse. If you have a legal right, if you're protecting citizens, employees, civil servants or otherwise, people need to be able to access the systems. People need to be able to file a complaint and not worry about repercussions or reprisals.

From my standpoint as a regulator, that's important. It's important that you're not creating these disincentives for individuals to file complaints, because, at the end of the day, this is all being done in the public interest and with the mandate of Parliament.

The Chair: Thank you, Ms. Mathyssen.

Mr. Bezan, you have four minutes.

Mr. James Bezan (Selkirk—Interlake—Eastman, CPC): Thank you, Mr. Chair.

For clarification, Mr. Dufresne, you said your office was created in 1983 under PIPEDA. That's the same legislation that was used to create the Office of the Information Commissioner as well.

Is that correct?

Mr. Philippe Dufresne: It was not PIPEDA. It was the Privacy Act.

Mr. James Bezan: It was the Privacy Act. Okay.

However, the Information Commissioner has the power to take the department and the Minister of National Defence to court for failure to comply with access to information.

Mr. Philippe Dufresne: That's right. The Information Commissioner was created under the Access to Information Act, and the Privacy Commissioner under the Privacy Act. More recently—I think it was 2017, but I may be wrong on the date—Bill C-58 amended the Access to Information Act to give the Information Commissioner order-making powers. That's something that has not been done yet for privacy.

Mr. James Bezan: You don't have the ability to hold the department, minister, deputy minister or chief of the defence staff accountable for failure to comply with the act.

Mr. Philippe Dufresne: I will not minimize the impact of a public ruling, a public recommendation or the role of committees and so on. However, I don't have the ability to issue a binding order.

Mr. James Bezan: Okay. That's one of the recommendations we should be looking at.

The other part of that is this: You mentioned people wanting to get access to their own records for their own needs at the Canadian Armed Forces or Department of National Defence, and having to go to court.

Do you think it's fair for one person to have to take on the entire Department of National Defence?

Mr. Philippe Dufresne: Well, I think a more efficient and accessible system is one where you can have a regulator issue an order. That order is then binding. Again, I don't—

Mr. James Bezan: That's not happening right now.

Mr. Philippe Dufresne: We don't have that right now.

Also, having the possibility of an order makes it more likely, in my view, that you're going to get early resolution on the matter without having to go through the process.

Mr. James Bezan: We've heard from multiple witnesses already, including the ombudsman, the former ombudsman Gary Walbourne, Mr. White and Mr. Drapeau. There is a culture of over-classification within the Canadian Armed Forces and Department of National Defence.

Do you think that's done to intentionally hide records from their own members and veterans?

● (1750)

Mr. Philippe Dufresne: I think the legislation provides certain exceptions for disclosure, either under my legislation—the Privacy Act—or the Access to Information Act. Departments have leeway with that. There are some valid public interest reasons to prevent disclosure under legislation, but recourse exists to challenge those.

Mr. James Bezan: I'll give the rest of my time to Mrs. Gallant.

Mrs. Cheryl Gallant (Renfrew—Nipissing—Pembroke, CPC): How often are military personnel system records audited for unauthorized searches?

Mr. Philippe Dufresne: I have statistics of the complaints we receive at my office. We receive complaints directly from Canadians. I've indicated that, I think, in the last five years, we've received 300 complaints.

Mrs. Cheryl Gallant: All right.

What is the privacy policy with respect to military personnel health records and access to those records by VAC?

Mr. Philippe Dufresne: Regarding access by VAC, there is some exchange of information between the two institutions in terms of those types of records. We have been engaged. We've been consulted on that. I understand we've received some PIAs, privacy impact assessments, on that.

Mrs. Cheryl Gallant: Troops returning from a deployment on commercial aircraft have had to complete the ArriveCAN app. We know the disclosure allows the app to share information to contractors working for Public Health, Services Canada, provincial, territorial or municipal...and may be used for program evaluation and other organizations.

Do we know whether or not any of our troops' personal or health information has been shared with commercial companies, state-owned enterprises or anyone at all outside our government?

Mr. Philippe Dufresne: We are currently investigating the ArriveCAN app following complaints, so I won't be able to speak further on that, as this is ongoing.

The Chair: Thank you, Mrs. Gallant.

Ms. Lambropoulos, you have the final four minutes.

Ms. Emmanuella Lambropoulos (Saint-Laurent, Lib.): Thank you, Chair.

Thank you, Mr. Dufresne, for being here with us today.

I'm wondering if you could tell us, based on the complaints you've received and the fact that some cases take a very long time to get a response or be dealt with, what you think would make the process more user-friendly. What is it that you think would help facilitate things or make it more accessible to people?

Mr. Philippe Dufresne: I think that the resources and efforts have to be put into making the system as user-friendly as possible. There are a number of modernization recommendations that need to happen in terms of making the principles of the system more up to date. An order-making power is one. A mandatory privacy impact assessment is another. There are some definitions, perhaps, that need to be updated as well.

Speaking for the privacy purview, one thing I've been highlighting since I started in this role is the need to treat privacy as a fundamental right, giving it that priority and making sure these matters are seen for what they are. These are individuals looking to have fundamentally important information about themselves. We need to make sure the system is accessible.

Ms. Emmanuella Lambropoulos: Do you find that the way the current system works is easy to understand for all users?

Mr. Philippe Dufresne: I think we can make it easier to understand and faster. We are seeing that in terms of the statistics, so that's something we're working towards.

Ms. Emmanuella Lambropoulos: How do you measure success in your work? What do you think could be done to improve? What shortcomings are there and how can we improve them, in general?

Mr. Philippe Dufresne: We're measuring success by looking at the statistics and trends and by trying to see whether the number of complaints is increasing and being resolved quickly. Are the timelines decreasing? Is the collaboration we see, the exchanges with the departments...? When we're thinking about privacy impact assessments, are those being done before new programs are started? Are we being kept informed and consulted? All of those things are elements of what we would look at in terms of success.

The Chair: Thank you.

On behalf of the committee I want to thank you both. Both of you are very sophisticated witnesses and know the time constraints that we have on committee, but thank you for your testimony. I appreciate your appearing under the circumstances.

Colleagues, before we gavel to an end, may I have Mr. Bezan move the subcommittee report? Ms. Lalonde will second it. Is there any debate?

(Motion agreed to [*See Minutes of Proceedings*])

The Chair: I have Mr. Bezan moving $16,500 for the defence committee report. It has been moved and seconded. Is there any debate?

(Motion agreed to [*See Minutes of Proceedings*])

The Chair: Finally, please indicate to me whether you will be available for meeting with the German defence minister on Friday, May 10, at 12:15 p.m. I have one Conservative, one NDP, one....

With that, I thank you. I appreciate your co-operation.