HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

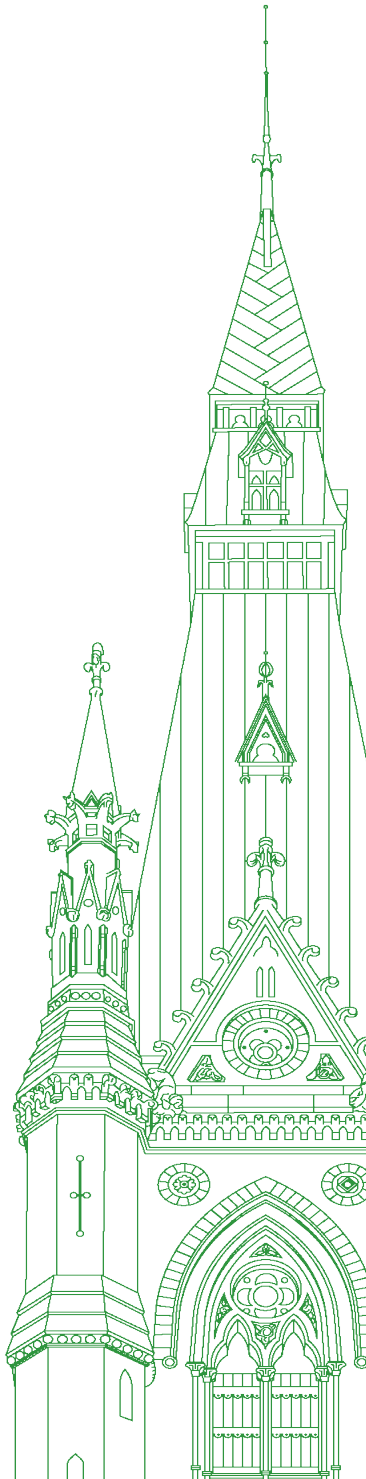
44th PARLIAMENT, 1st SESSION

Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 087

Wednesday, October 25, 2023



Chair: Mr. John Brassard

Standing Committee on Access to Information, Privacy and Ethics

Wednesday, October 25, 2023

● (1650)

[*English*]

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

Good afternoon, everyone.

[*Translation*]

Welcome to meeting no. 87 of the House of Commons Standing Committee on Access to Information, Privacy and Ethics.

[*English*]

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

I would like to make a few comments before the business of the committee starts, for the benefit of witnesses and members.

Please wait until you are recognized by name before speaking.

For those participating by video conference, click on the microphone icon to activate your mike, and please mute yourself when you are not speaking.

Those on Zoom have the interpretation choices, at the bottom of their screens, of “floor”, “English” or “French”. Those in the room can use the earpiece and select the desired channel. Although the room is equipped with a powerful audio system, feedback events can occur. These can be extremely harmful to the interpreters and cause injuries.

I remind you that comments from members should be addressed through the chair.

[*Translation*]

Today, we have the same witnesses for two hours, to talk on two different topics.

For the first hour, pursuant to Standing Order 108(3)(h), we will receive a briefing on the annual report and other reports of the Privacy Commissioner.

Then, for the second hour, the committee will resume its study on the use of social media platforms.

[*English*]

I would now like to welcome our witnesses today.

From the Office of the Privacy Commissioner of Canada, we have Mr. Philippe Dufresne, Privacy Commissioner of Canada, and Mr. Michael Maguire, director, Personal Information Protection and Electronic Documents Act compliance directorate.

Welcome, gentlemen, to the committee.

Commissioner, you have five minutes to address the committee. Please go ahead, sir.

[*Translation*]

Mr. Philippe Dufresne (Privacy Commissioner of Canada, Offices of the Information and Privacy Commissioners of Canada): Good afternoon, Mr. Chair.

Good afternoon, members of the committee.

I am pleased to be here today to discuss my 2022-23 Annual Report to Parliament, which highlights the important work that my office is doing to protect and promote the fundamental right to privacy in a time of unprecedented technological change.

It is encouraging to see this continued focus on the importance of privacy, as it impacts virtually all aspects of our lives.

Many of the public interest issues that you are seized with as parliamentarians—children's rights, online safety and cybersecurity, democratic rights, national security, equality rights, ethical corporate practices and the rule of law—all have privacy implications and, I would argue, all depend on strong privacy protections.

[*English*]

In this digital era, as you will see from some of the work and investigations my office has conducted this year, routine activities of daily life—for example, socializing online, using mobile apps, getting packages delivered or going to the checkout counter—can also raise privacy issues.

Since my appointment as Privacy Commissioner in June 2022, I've identified strategic priorities for my office that helped frame our work over the past year and that will guide the way ahead. These include addressing the privacy impacts of the fast-moving pace of technological advancements—especially in the world of artificial intelligence and generative AI—protecting children's privacy, and maximizing the OPC's impact in fully and effectively promoting and protecting the fundamental right to privacy.

[*Translation*]

To support these priorities, this past year we have engaged extensively with our domestic and international counterparts to identify and undertake collaborative opportunities.

We have also continued to advocate domestically for the modernization of Canada's privacy laws. I was honoured to appear before the Standing Committee on Industry and Technology last week in the context of their study of Bill C-27, the digital charter implementation act, 2022, where I made 15 key recommendations needed to improve and strengthen the bill. I was pleased to see a number of them endorsed by Minister Champagne in the form of amendments that will be put forward to the committee, and I look forward to the work of Parliament in reviewing this important bill.

[*English*]

I will now turn to some of our compliance work from the last year.

We accepted 1,241 complaints under the Privacy Act, representing an increase of 37% over the previous year, and 454 under the Personal Information Protection and Electronic Documents Act, or PIPEDA, a 6% increase over the year before.

One of the public sector investigations highlighted in this year's report involved Canada Post's Smartmail marketing program. Our investigation revealed that Canada Post builds marketing lists with information gleaned from the envelopes and packages that it delivers to homes across Canada. It makes these lists available to advertisers for a fee. We found this contravened the Privacy Act, as it was done without the knowledge and consent of Canadians. We recommended that Canada Post stop its practice of using and disclosing personal information without first seeking authorization from Canadians. As a possible solution to remedy this matter, we recommended that Canada Post send a mail notice to Canadians to inform them of this practice and indicate an easy way for Canadians to opt out.

Until the tabling of my annual report, which made this decision public, Canada Post did not agree to implement this solution. After the report was made public, Canada Post issued a statement that it would review its policies. I expect Canada Post to comply with the Privacy Act and I look forward to hearing from them on the next steps to resolve this matter.

[*Translation*]

The report also highlights some of our private-sector investigations from last year, including our investigation of Home Depot's sharing of the personal information of customers who opted for an electronic receipt instead of the printed one at checkout with a social media company.

Home Depot has since stopped that practice and implemented my offices recommendations. This case underscored the importance of businesses obtaining meaningful consent to share customers' personal information.

Another important area of our work is addressing breaches in the public and private sectors.

We remain concerned about possible under-reporting of breach incidents in the public sector. The number of reported breaches fell by 36% to 298 last year, and only one of those reports involved a cyber-attack. This compares to 681 breach reports from the private sector, of which 278 were cyber-related.

● (1655)

[*English*]

We also engage in groundbreaking policy work, provide advice and guidance to organizations in both the public and private sectors on privacy matters of public interest and importance, and continue to provide advice to Parliament.

We know that privacy matters to Canadians more today than ever before and that they are concerned about the impact of technology on their privacy. Our latest survey of Canadians found that 93% have some level of concern about protecting their personal information and that half do not feel that they have enough information to understand the privacy implications of new technologies. This is why the work of my office to deliver concrete results that have meaningful impacts for Canadians and privacy in Canada is so important.

In closing, I would like to thank this committee for its work over the years, including the many reports and recommendations in the field of privacy. I cite them often. We certainly consider and consult them very often, and I know that Canadians do as well.

I look forward to continuing our efforts to ensure that privacy rights are respected and prioritized by government institutions and businesses alike, and to position Canada as a global leader on privacy.

I would now be happy to answer your questions.

[*Translation*]

Le président: Thank you for your speech, Mr. Dufresne.

Before we go to questions, I'd like to welcome a new analyst who will be working with the committee, Maxime-Olivier Thibodeau. He joins Alexandra Savoie.

Thank you and welcome, Mr. Thibodeau.

Will begin our questions with Mr. Barrett.

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

[*English*]

Mr. Michael Barrett (Leeds—Grenville—Thousand Islands and Rideau Lakes, CPC): Thanks very much, Mr. Chair.

Commissioner, thank you for joining us. Mr. Maguire, thanks very much as well.

I would like to take a moment to address Monday's committee meeting.

We had a different commissioner here. We had the commissioner of the RCMP to address a serious issue. Before the meeting got under way, we had the Liberal vice-chair move to adjourn the meeting. It was an incredibly important topic; we had the commissioner of the RCMP here to address concerns that were raised in the media last week with respect to the Prime Minister's SNC-Lavalin scandal. This is where the Prime Minister was found guilty of breaking Canada's ethics laws and—

The Chair: Mr. Barrett, we have Mr. Dufresne here, so if you want to keep it relevant, please....

Mr. Michael Barrett: Yes. Thanks very much, Mr. Chair.

We have a Prime Minister who broke Canada's ethics laws. The RCMP requested documents, and the Prime Minister used cabinet confidentiality to obstruct the release of those documents. This is an issue that we're going to have to revisit at this committee. It's of high importance to Canadians that they're able to have confidence in their democratic institutions, and no one is above the law, including the Prime Minister.

That said, Mr. Dufresne, I appreciate your opening comments, particularly with respect to the Crown corporation, Canada Post. I think that all Canadians expect it to follow the Privacy Act. I am heartened that following your investigation into Home Depot, they complied with your instruction. While I understand that Canada Post is reviewing the situation, it's very clear that they should also comply with your instruction.

Have you been made aware of instances in Canada of people's data being scraped and collected by foreign governments for nefarious purposes?

Mr. Philippe Dufresne: We have issued some investigations. One involved Clearview AI, an organization that was scraping the images of Canadians online and creating what was described as almost a permanent lineup of facial identification. We found that this was a violation of the privacy legislation and made recommendations to the organization. The organization ultimately decided to depart Canada. That was a high-profile instance of a concern.

We are continuing to monitor the situation with international colleagues. We have recently issued a statement on data scraping, calling upon social media organizations to take steps to protect the information, to inform and to have some measures in place. We also highlighted some steps that individuals can take as well.

It is something that we are certainly focused on.

● (1700)

Mr. Michael Barrett: Is it a reasonable concern of Canadians that their personal information or biometric data could be taken from social media platforms and then used by foreign state actors, hostile foreign governments, to perpetrate intimidation on diaspora communities from those countries?

I want to be specific. There are concerns, which are well known, about the national security law passed by the dictatorship in Beijing that are germane to the company ByteDance, which owns TikTok. This is an issue about a very popular social media app, and people are concerned about the risks to their privacy and personal information. We have seen governments suspend the use of this app on government devices.

How concerned should people be about using this app on their personal devices, or about their children using it on their personal devices?

Mr. Philippe Dufresne: There are two things, Mr. Barrett.

In our statement dated August 24, 2023, we talked about some of the privacy risks in terms of data scraping. Some of them include targeted cyber-attacks, identity fraud, monitoring, profiling and surveilling of individuals, unauthorized political or intelligence-gathering purposes, or unwanted direct marketing or spam.

There are a number of risks, which is why we are calling on social media companies, and indeed all organizations, to respect privacy obligations. We set out a number of ways in terms of risk mitigation techniques that social media companies can and should take to protect that information from bad actors that would scrape the information.

We also, again, highlight some practices and advice to individuals, although it is not on individuals to protect themselves exclusively: The organizations have a duty, and there is advice that can be taken.

You made reference to TikTok. I initiated a commissioner-initiated complaint with respect to TikTok last year. We initiated this in February—this is a joint investigation—and I am moving forward with my provincial colleagues from Quebec, Alberta and British Columbia. We initiated that to look at the privacy practices. We are looking forward to completing this investigation, hopefully, by the end of March 2024.

Mr. Michael Barrett: With about 30 seconds left, I hope we have the opportunity to come back to your strategic goal of protecting children and finding out more about how you plan to do that, and any examples you have uncovered with respect to children being targeted or manipulated, particularly by social media apps or companies with respect to foreign state actors.

I think that's close to the end of my time. Thank you very much.

The Chair: Thank you, Mr. Barrett.

Next we will go to Madam Fortier

[*Translation*]

Ms. Fortier, you have the floor for six minutes.

Hon. Mona Fortier (Ottawa—Vanier, Lib.): Thank you, Mr. Chair.

Before I put my questions to Mr. Dufresne, I too would like to clear up a few things.

On Monday, I believe that the Chair abused his authority. I'd like to remind him of certain procedures and regulations that I believe were not followed.

[*English*]

You know that there are long-standing procedures and practices that govern the House of Commons standing committees. The process for undertaking subject matter studies, the process for moving motions and the role of the chair are outlined in the *House of Commons Procedure and Practice*. That is what I debated during the suggestion and motion to adjourn the meeting.

I will remind us that page 1061 of the third edition of *House of Commons Procedure and Practice* states:

> A motion is needed to submit a proposal to a committee and obtain a decision on it. A motion is moved by a member to have the committee do something, order its Chair and staff to ensure that something is done (an order) or express an opinion on a matter (a resolution).

Page 1011 of the same edition states:

> The committees then undertake to define the nature and scope of the study, to determine how much time they will devote to it and whether or not they will report their observations and recommendations to the House.

The Chair: Madam Fortier, excuse me for a second. I'm going to excuse—

Hon. Mona Fortier: I'm almost done.

The Chair: I called Mr. Barrett on relevance before and I'm going to do the same thing to you.

We have Mr. Dufresne here to talk about his report, so I'm going to give you a little more latitude, but—

Hon. Mona Fortier: I'm almost done. Thank you very much, Chair.

Lastly, page 1039 states that the chair calls meetings and decides on the agenda for the meeting in compliance with instructions from the committee.

The process outlined above was not followed in the circumstances of the meeting scheduled for October 23, 2023. Therefore, I cannot wait for us to debate that motion, and then we will be able to resolve what happened last Monday.

● (1705)

[*Translation*]

Thank you for allowing me to share my thoughts with you as well.

Having said that, thank you very much for being with us today, Mr. Dufresne. I'm happy to see you in person and to have the privilege of congratulating you on your appointment to this position. I know you were appointed some time ago, but I'm very happy to see you in this position.

You mentioned that you had a backlog of complaints that needed to be dealt with, and that it was starting to put a strain on your resources.

What course of action or approach are you thinking of taking? From what I understand, your organization's work is becoming increasingly complex, particularly in terms of automation.

I'd like you to tell us about the complexity.

Mr. Philippe Dufresne: Thank you very much, Ms. Fortier. I'm happy to see you in person as well.

We addressed this issue early in my term, because it's important that we make quality decisions, but how fast we make them is equally important. Decisions must be delivered within a reasonable timeframe. However, when too many requests are received, it takes longer to respond. We've therefore identified a need and obtained additional resources from Parliament. We're grateful for that.

We're looking at this issue from all angles. We're reviewing our internal processes to determine whether we can operate in a more agile way, whether we're adequately managing risk, whether we can use other technologies, and whether we can use incentives to encourage organizations to resolve disputes more rapidly, for example. I'm a big believer in voluntary dispute resolution.

To improve efficiency at the Office of the Commissioner, I've had a lot of discussions with industry and government representatives to understand the barriers and benefits. One thing I'd like to do is recognize the government's or industry's good work when it comes to privacy, not just their shortfalls, to encourage them to continue moving in the right direction.

There are many opportunities to improve efficiency at the Office of the Commissioner, but it certainly remains one of the main challenges. That's why our efficiency is one of my three strategic priorities, along with technology and protecting children's privacy.

We're really going to do everything we can to improve the way we operate. We've already started to see an improvement.

Hon. Mona Fortier: You piqued my curiosity during your testimony. You stated that some businesses in the private sector don't report privacy breaches.

Could you explain to the committee what that means? Can you suggest any solutions? For example, should the Privacy Act or the regulations be amended?

Mr. Philippe Dufresne: Yes, for the moment, privacy breaches in the public sector are reported in accordance with Treasury Board directives. There's a legal obligation in the private sector. We definitely have recommendations on the subject. I think it's useful to have binding legal obligations because that encourages organizations to take action. We need them in both the public and private sectors.

However, I also think it's a matter of understanding and communication. You have to understand the criterion for reporting privacy breaches. Sometimes organizations acting in good faith have a poor understanding of that criterion or else underestimate the risk of harm.

We saw this in some of our investigations this year. Some organizations indicated that they hadn't reported a privacy breach because they thought the risk of harm wasn't high enough. In some cases, we disagreed and determined that there had been a risk of financial harm, reputational harm or disclosure of sensitive information.

Consequently, we have some work to do to increase awareness, and we have to make sure we have the necessary tools for that purpose. However, we will continue working on this and encourage organizations to look into these issues. When they report breaches to us, we can offer them opinions and advice and work with them. That's really our objective.

We also work with citizens because we have to find solutions to protect the victims of those breaches.

Hon. Mona Fortier: Thank you.

The Chair: Thank you, Mr. Dufresne.

Thank you, Ms. Fortier. Thanks as well for your comments.

Mr. Villemure, you have six minutes.

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

Mr. Dufresne, thank you for being with us today. I carefully read your report, which I consider remarkable.

As I read it, I wondered what your current concerns are for the future of privacy. People in my riding talk to me about this at great length. I would also say that the risks are changing.

What are your concerns?

● (1710)

Mr. Philippe Dufresne: One of the things I think about is how to communicate with citizens more effectively. What you've done in your riding with your seminars and discussions is very good, and it's a good step in the right direction.

We have to get to a point where Canadians understand what's happening, and we have to equip them to do that. Technology advances very quickly. You can see that with generative artificial intelligence, and other technologies will emerge. Sometimes Canadians may feel confused about it all because everything changes so quickly.

What can we do about it? Sometimes I hear people say it's too late to protect privacy because everything's moving too fast, and they give up. If there's one thing that I consider a concern, it's that.

I think it's important to tell people that we have to protect privacy, that it's possible to do so, that institutions can do it and that people can do it as well. Statutes will never be amended as quickly as technology evolves. The same is true of the regulations the government makes.

However, we need to pass legislation based on principles that can be applied to new technology. I'm a real believer in privacy risk assessments and in making them an obligation. I'm a true believer in transparency and in communicating more and more effectively with Canadians about what can be done with their information and how it will be used.

Consent provisions are often very hard to understand, even for experts. Consequently, people grow tired of it all. In the investigations I discuss in my report, whether they concern Canada Post, Home Depot or Tim Hortons, people are sometimes surprised by what's done with their information.

In our discussions with organizations, we asked them to be proactive and to make that information readily accessible. Sometimes their response is that their information is provided in the privacy policy on their website or at the post office. Then we tell them that they're asking Canadians to bear the burden of searching for that information when those organizations are in a better position to communicate it than they are.

Mr. René Villemure: I'm interested in that point because, when you go onto a website, such as the Canada Post website, for example, you often consent to your information being used, thinking that nothing serious is likely to happen because it's Canada Post after all. However, most of the people I meet and who attended the artificial intelligence seminar told me they didn't understand the purpose of consent. Ultimately, you may give your consent to La Presse or RDS, but the actual purpose is rarely clear.

What can we do about it?

Mr. Philippe Dufresne: I think we have to hold public discussions, be transparent and have obligations to be transparent.

The phenomenon you're describing has accelerated even more with artificial intelligence. We may think we know our personal information will be used by such and such an entity. However, do we really know what anyone can conclude about us based on that information? What inferences can be drawn? Sometimes postal codes or tastes in music, for example, can help someone deduce a person's sexual orientation, income level and so on. People don't know all that.

I recommended that Bill C-27 provide for a transparency obligation so that, when people reached a decision with the help of artificial intelligence, they could request an explanation in every case. However, the current version of the bill provides that a general account may be provided only in cases that would have a significant impact on the individuals concerned. I recommended that part be deleted because, for the moment, I think it's better to encourage more transparency rather than less.

We have to try to find pleasant ways to explain this. One of my mandates is to try to acquire tools. We provide a lot of information on our website, and we try to explain it all as best we can, but I think we can do better.

We also have to talk about children, because I think the message has to be adapted to suit the audience.

Mr. René Villemure: It seems to me we hear more and more people saying that the toothpaste is unfortunately out of the tube. So they wonder what they should do now. Should they waive their privacy?

What can they expect with regard to privacy?

Mr. Philippe Dufresne: I think you should never waive your privacy because it's a fundamental right. We have to remind people that privacy has no transactional or commercial value that can be sold and that, if you get something exciting enough in return, such as innovation, that's worth it. It's a fundamental right that defines us as individuals and that other rights are based on, rights that enable us, for example, to be free, to have democratic systems and equality and to be free from discrimination. It's an extremely important right. People and institutions must be reminded how important it is.

The idea isn't to say there'll be no innovation. When I was appointed to my position, I said that the right to privacy was a fundamental right but that it also had to support innovation and the public interest, and that that was possible. Sometimes it requires a little more work, as is the case with equality, but it requires less work if you act right away.

We absolutely must tell people that the toothpaste isn't out of the tube and that, if some of it is, we'll put it right back in because it's important that we do so. We'll get there by working together.

● (1715)

Mr. René Villemure: Thank you very much.

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

Mr. Boulerice, welcome to the committee. You have the floor for six minutes.

Mr. Alexandre Boulerice (Rosemont—La Petite-Patrie, NDP): Thank you very much, Mr. Chair.

I'd like to thank Mr. Dufresne for taking part in our important study.

Mr. Dufresne, I learned something recently that really struck me.

You just said that updates to laws and regulations will never be able to keep up with technological advances. We agree on that.

Two years ago, the Department of Justice conducted an online public consultation on the modernization of the Privacy Act. However, there have been no major updates to the act since it was adopted in 1983. In 1983, when I was 10, we used floppy disks and I watched movies on VHS tapes.

In your opinion, how urgent is it to modernize the Privacy Act?

Mr. Philippe Dufresne: I think it's absolutely essential to modernize this act. We also need to modernize the part of the Privacy Act that deals with the private sector. This law is 20 years old, so it's older than Facebook and social media. It is positive that Bill C-27 aims to modernize the act with respect to the private sector. I look forward to seeing this bill move forward.

In addition, I hope that a bill to modernize the act for the public sector will soon follow. The Minister of Justice had said, when Bill C-27 was tabled, that the public sector privacy bill would follow. Consultations were held with first nations and indigenous peoples on certain implications. The Department of Justice published a report on these consultations—I believe it was in September. The work is ongoing. In my opinion, the solution is to move forward with Bill C-27. The model passed in this legislation can then be adapted to the public sector, as needed. That could be beneficial.

Among our proposals, we suggest that there should be an increasing number of public-private partnerships and that the government should work hand in hand with the industry. At present, we have two laws with different requirements for government and the private sector. This is not optimal, and it creates problems in terms of interoperability. I entirely agree with you that this is becoming important.

In the meantime, the law applies, and our office will continue to implement it to the best of our ability. In fact, this is a message that my counterparts from the G7 countries and I conveyed when we were in Tokyo last summer. At that meeting, we talked about artificial intelligence. To address people's concerns, we said we needed laws on artificial intelligence. There are already some—privacy laws, for instance. They exist and they are enforced.

I've also launched an investigation into ChatGPT, to confirm whether or not it is compliant with the legislation. Tools do exist, but they absolutely must be modernized. We will be there to support Parliament.

Mr. Alexandre Boulerice: You can make recommendations, but you do not have the power to issue orders.

Do you think that should be required? What benefits could come of the power to issue orders?

Mr. Philippe Dufresne: The power to issue orders is very important. In my view, the ideal scenario is not having to use that power, but its mere existence will encourage good decision-making. I say this as commissioner, but also as a senior corporate executive and as an employer: When there are a lot of priorities and a lot of pressure but little time and few resources, organizations prioritize binding legal obligations over recommendations. That is standard.

I don't want a right as fundamental as privacy to be treated as if it were nothing more than an asset. That said, organizations often do treat it that way.

I can use my power to make recommendations, but it would also be very important for me to have the power to issue orders.

● (1720)

Mr. Alexandre Boulerice: In your office's report entitled “Protecting Privacy in a Pandemic,” you mentioned that three departments had refused to implement your recommendations: Treasury Board, the Department of National Defence, and the Border Services Agency.

Has anyone given you any explanation or justification for this?

Mr. Philippe Dufresne: Certainly. There are sometimes discussions about that.

As for the cases you're referring to, sometimes a department tells us it's already doing what we recommend. In the case of the pandemic, we also carried out an assessment of proportionality and necessity, which is not mandatory under the Privacy Act, but which we feel should be. We put forward that analysis.

It's a dialogue. We are always given the reasons for refusal, and dialogue is established.

Some breaches are more serious than others. The really worrying situations are those where there has actually been a major breach or a major consequence, combined with a complete refusal to follow our recommendation. That can undermine trust.

I feel the power to issue orders is important. When an officer of Parliament makes a recommendation to an organization and the latter refuses to implement it, the situation is not satisfactory. I believe there must be sufficient justifications given. If we had the power to issue orders, this wouldn't be a problem. We'd issue them when necessary. With that said, in my opinion, they should only ever be used exceptionally.

The same applies to fines. In Bill C-27, we would add the possibility of imposing significant financial penalties on organizations. I think this is very important, for the same reason again: to create incentives. The idea is not to use them often, but...

Mr. Alexandre Boulerice: They would be deterrents.

Mr. Philippe Dufresne: That's right.

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

That's the end of our first round of questions. We'll now begin the second round.

Mr. Gourde, you have the floor for five minutes.

Mr. Jacques Gourde (Lévis—Lotbinière, CPC): Thank you, Mr. Chair.

Thank you for being here, Mr. Dufresne.

In your opening statement, you talked about working with the provinces and other countries. I'd like to talk about the province of Quebec.

Quebec has already enacted law 25, an act to modernize legislative provisions as regards the protection of personal information. Does that law have more teeth than the current federal laws? Do you work with Quebec? Tell me where things stand, if you wouldn't mind.

Mr. Philippe Dufresne: Yes, Quebec's law 25 definitely has more teeth than existing federal laws, simply because it grants the power to issue orders. Quebec's access to information authority, the Commission d'accès à l'information, or CAI, can issue binding orders and impose heavy fines, similar to the European model under the General Data Protection Regulation. That makes it a more robust piece of legislation on that front. It lays out proactive obligations.

Hopefully, Bill C-27 will make its way successfully through Parliament and bring federal laws more up to date in that regard. It's not exactly the same as law 25, but it comes close with the power to issue orders, and to impose fines as well as proactive obligations on companies. I think it's a good model, following in the footsteps of Europe and Quebec. I think, federally, we can get there.

To answer your question about working with the CAI, I can report that we do indeed work very closely with Quebec and all the provinces and territories.

I was in Quebec City in September for the annual gathering of federal, provincial and territorial privacy commissioners, which the CAI hosted. We had some very important and useful conversations. We put out two resolutions, including on the protection of young people's privacy. They are joint statements reflecting principles that all the commissioners have agreed upon, despite the legislative differences between the jurisdictions. In this way, the commissioners are trying to make things easier for companies by flagging common elements across the different regimes. My office carries out joint investigations with provinces that have regimes similar to the federal government's, so Quebec, Alberta and British Columbia. We worked together on the investigations into TikTok, ChatGPT and Tim Hortons.

Our collaborative work is not only extensive, but also very useful. We are able to make sure that we are on the same page across the country.

● (1725)

Mr. Jacques Gourde: I have a quick technical question.

Are federal institutions in Quebec subject to Quebec's law? My riding office is one example.

Mr. Philippe Dufresne: Federal privacy laws apply everywhere in Canada, except in provinces whose legislation is similar to the federal government's, which is the case in Quebec.

Any activity taking place solely in Quebec is governed by Quebec's legislation, but many issues have an impact beyond Quebec's borders, especially those involving the Internet and social media. That's why we work together so closely and often conduct joint investigations. We're able to cover everything that way.

Mr. Jacques Gourde: I'm going to switch topics now. People are worried about their privacy. Nowadays, with social media and such, they have reason to be concerned. I'll give you a trivial example. If my spouse and I talk about taking a trip, travel ads will show up on my feed, when I haven't done any searches related to travel. It's as though my phone is registering what I talk about. It's clear that AI is at work and everything we say is being listened to, but it's far-reaching. If my son and I talk about trucks, I'll get ads for trucks on my feed.

Mr. Philippe Dufresne: That illustrates why it's important for the organizations making those ads appear to be more transparent, to comply with proactive obligations and to say why they are doing what they're doing. You should have the right to ask the organization why that ad showed up for you.

You bring to mind something important, Mr. Gourde. Just because information is publicly available online doesn't mean it's not personal information that is supposed to be protected. I think there's a misunderstanding about that. The thinking is that it's not personal information because it's on the Internet, but the law still applies. There is an exception for public information, but it's very limited and it has to be defined in the regulations.

Generally speaking, you're still protected in that regard.

Mr. Jacques Gourde: Is it a thin line when it comes to profiling? Is it legal or illegal?

Mr. Philippe Dufresne: We explicitly recommended that the term “profiling” be included in the definitions. When organizations use an algorithm, when they infer things from your personal information and, then, use that to build profiles, there are consequences, and they need to be taken into account and regulated. Both Quebec's law and the European regulation refer to the term “profiling”. My office recommended it be explicitly included in Bill C-27.

Mr. Jacques Gourde: Thank you.

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

[*English*]

Mr. Bains, you have five minutes. Please go ahead.

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

Thank you, Monsieur Dufresne and Mr. Maguire, for joining us today.

Monsieur Dufresne, in May 2023 your office announced that it was appealing the Federal Court's decision regarding Facebook's possible contravention of PIPEDA, noting that “issues at the heart of the case are directly related to fundamental privacy rights of Canadians” and that the issues would “benefit” from being clarified by the Federal Court of Appeal.

Has there been any progress there?

Mr. Philippe Dufresne: There has been progress. It is making its way through the Federal Court of Appeal process. We have filed our factums, our written representations, to the Federal Court of Appeal. Facebook has filed its written representation. Next steps will be to wait for the court to set a hearing date, which we hope will take place in the coming months and, following that, oral arguments and then a decision.

Mr. Parm Bains: Okay.

Your annual report notes that the Office of the Privacy Commissioner has developed various strategies to promote efficiency gains that include “exploring options for automation to help staff work more efficiently”. Have any of the office processes been automated?

Mr. Philippe Dufresne: We've not automated processes. I'm looking to my colleague, Mr. Maguire.

We've been looking at a first step in terms of systems efficiencies, in terms of risk management profiles, in terms of.... We've developed a tool to identify real risk of significant harm in the case of breaches, so that's an automated process. We're obviously carefully monitoring AI and generative AI.

We did make the decision that for the moment—because we are investigating ChatGPT and hoping to conclude that investigation in the coming months—we are not using that tool at the OPC for the moment, but we will be considering, obviously, appropriate uses of any tools that could assist us, again making sure that they are privacy compliant.

● (1730)

Mr. Parm Bains: You've already stated that ChatGPT is at risk here and that you're studying it now. Considering that there are so many different versions of ChatGPT or other AIs like it, are you looking at any others?

Mr. Philippe Dufresne: For the moment, we are investigating OpenAI and ChatGPT, but again, when we do these investigations, we try.... If we identify lessons or principles, they can assist, hopefully, and can guide other organizations.

For instance, in the Home Depot decision, while we made our conclusion specific to Home Depot, this was a practice that was being used in the industry. When I made my report public, I called on other organizations, any organizations that would be using a similar practice of sharing information when Canadians asked for an email receipt instead of a printed receipt, and I said that this is against privacy law and it needs to stop. A number of organizations were identified as having that practice. We reached out to them, and a great many have stopped, if not all.

That is a systemic impact that we look to have as well, even if we're dealing with one specific case.

Mr. Parm Bains: You mentioned working with Quebec and others. There's the Global Privacy Assembly. Can you maybe elaborate on how participating in those international bodies improves...?

Mr. Philippe Dufresne: Certainly, and thank you for the question. We talked about that in the annual report.

There is a very strong active domestic—federal-provincial-territorial—Canadian community, but also internationally there are a number of groups. I've been very active with the G7 round table of data protection authorities. Data protection authorities are essentially privacy commissioners from the G7 countries. We meet annually. We met a year and a half ago in Bonn, Germany. This year we met in Tokyo. One of the key themes of that group has been that we need to have cross-border data flows to ensure that we can have strong international trade when data is travelling from jurisdiction to jurisdiction. How do you ensure that it's protected and safe?

There are number of tools—legislative tools, contractual programs and so on. We have discussions on that. AI has been a growing topic. Last June in Tokyo we issued a statement about our expectations. I think it was one of the first statements in which privacy commissioners set out our expectations for AI from a privacy perspective. We said, for one thing, that current laws apply. Privacy law applies. It's not a legal void. We already have protections and we are going to apply them. We stated our expectation that organizations have privacy by design, that they have privacy impact assessments when developing these tools, and that they do this.

It was a call to action. I was happy to see, in the industry department's voluntary code of practice for AI that was launched a couple of weeks ago, that the G7 declaration was highlighted, as was a reminder that the Privacy Act continues to be important.

The Chair: That's wonderful.

Thank you, Mr. Dufresne. Thank you, Mr. Bains.

[*Translation*]

Now we go to Mr. Villemure for two and a half minutes.

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

I'd like to use my time to give notice of a motion.

Here it is:

> That, pursuant to Standing Order 108(3)(h), the committee undertake a study of the RCMP's decision not to pursue a criminal investigation into Prime Minister Justin Trudeau following the reprimand issued by the Conflict of Interest and Ethics Commissioner regarding his involvement in the SNC-Lavalin affair; that the committee devote three meetings to this study; that the committee request to appear, for one hour per witness: (a) the former Conflict of Interest and Ethics Commissioner, Mr. Mario Dion; (b) the Conflict of Interest and Ethics Commissioner, Mr. Konrad Winrich von Finckenstein; (c) the RCMP Commissioner, Mr. Michael Duheme; (d) Mr. Frédéric Pincince, International Investigations, Ontario Division; (e) representatives of the Royal Canadian Mounted Police in 2019 who may be involved; and, lastly, (f) the former advisor to the Prime Minister, Mr. Gerald Butts; that the committee report to the House; and that, pursuant to Standing Order 109, the committee request a comprehensive response from the government.

The Chair: Thank you, Mr. Villemure.

[*English*]

You're placing a motion on notice. Is that correct?

[*Translation*]

Mr. René Villemure: Yes, absolutely.

The Chair: I stopped the clock. You have two minutes and 26 seconds left.

Do you want to question the witnesses?

Mr. René Villemure: Yes, absolutely.

● (1735)

The Chair: We're listening.

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

My apologies, Commissioner, for that interruption.

You mentioned something earlier that brought back a lot of memories. You said that information isn't necessarily public by virtue of being online.

I'd like you to explain that statement, because it's a concept I don't think everyone grasps.

Mr. Philippe Dufresne: Absolutely.

Privacy laws apply to personal information, information that can identify us, because it has to be protected. That information can be used to draw a number of conclusions about us. The law sets out an exception: public information is not subject to certain obligations. Nevertheless, the exception has a very narrow definition. It has to be prescribed by regulation, and it's very limited.

Generally speaking, information that is online is public. Personal information, however, is still personal information. That means organizations are not allowed to use the information however they wish. They have to adhere to the applicable principles. That is the reason why we have investigated organizations that used excessive means to collect photos online to build facial recognition databases and, then, tried to sell them to police.

First, we conducted an investigation into the company Clearview AI, and we found that the database went way too far. There was no framework of restrictions, and the company did not set parameters with respect to necessity, proportionality and so forth.

Second, we conducted an investigation and tabled a special report to Parliament on the RCMP's use of the company at the time.

We found that the RCMP violated the act by using the company and failed to meet its own obligations. The RCMP has since stopped using the company and initiated the national technology onboarding program.

That is a very clear example of how information that appears online is still considered personal information.

Mr. René Villemure: That's a helpful clarification.

We learned a new word this week, spamouflage.

What concerns do you have around privacy and spamouflage?

The Chair: Please keep your answer brief.

Mr. Philippe Dufresne: Giving people false information, using information that appears to be true but isn't to mislead Canadians is a worrisome practice. That's why generative AI is worrisome. The OECD surveyed G7 ministers and put out a report. The thing that worried them most about AI was disinformation. Privacy was third. That underscores how important it is to protect privacy overall and to guard against disinformation.

The Chair: Thank you.

Mr. Philippe Dufresne: The OECD report is publicly available.

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

We now go to Mr. Boulerice for two and a half minutes.

Mr. Alexandre Boulerice: Thank you, Mr. Chair.

Mr. Dufresne, at the end of our discussion in the previous round, you talked about how your office applies the principles of necessity and proportionality. In your last report on privacy during the pandemic, you point out that the current law isn't satisfactory because those principles are not adequately reflected.

Can you explain all that? How far apart are the principles you want to see in place and the current law?

Mr. Philippe Dufresne: Yes, of course.

Under the Privacy Act, the public sector's obligations are less stringent than the private sector's. Departments are required to show that the information is used for purposes related to their respective mandates. For example, they have to show that they have a legal mandate to do X, so they can do it.

Some obligations are more specific, like those at issue in the Canada Post case. When an organization uses information indirectly, the obligation threshold is greater. It has to ask for permission. The first major consideration when a public organization uses information is whether the activity is relevant to its mandate.

We think it's important to impose the obligations of necessity and proportionality, in keeping with international principles and practices in the private sector. The idea is to consider what information the organization is collecting and for what purpose. It's a bit similar to how it works for charter human rights. Is the organization's purpose important enough? Will the measure achieve the purpose? Has the organization done everything possible to minimize the use of the information in achieving its purpose?

We underscored those principles in our report on the pandemic, and we apply them. While we realize they aren't binding, we apply them and use them to inform our recommendations. We've been able to draw some useful lessons. On the whole, the government adheres to the principles. Occasionally, we're of the view that there should have been more information on how the organization assessed the discarded options, but that, on balance, its decision was justifiable.

It's a standard that encourages decision-makers to ask questions about what they're doing and whether they are minimizing the risks. That's more or less what we are asking.

One of my major recommendations for Bill C-27 is to require organizations to conduct audits and privacy impact assessments, or PIAs. It's about considering what the risks are and which measures can minimize them.

PIAs are good for privacy, and they're good for Canadians.

● (1740)

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

We have a few rounds. The next members will have turns of five minutes, starting with Ms. Gladu, followed by Mr. Kelloway.

Go ahead, Ms. Gladu. You have five minutes.

[*English*]

Ms. Marilyn Gladu (Sarnia—Lambton, CPC): Thank you, Chair.

Thank you, Mr. Dufresne and Mr. Maguire, for being here tonight.

I want to start off with how I'm very disappointed that Canada Post was taking people's private information and selling it to others. I'm even more disappointed that when you pointed it out and asked Canada Post to stop, they didn't really do anything until the issue went public, and now they're just reviewing it.

Is there no remedy from you or the federal government that could make Canada Post stop taking people's private information and selling it?

Mr. Philippe Dufresne: This is why I recommended that I have the authority to issue binding orders, which I do not have under either the private sector or the public sector. What I have is the authority to make recommendations and to make those recommendations public. This is what I have used.

I was pleased to see the response from the public and parliamentarians. There is a question on the Order Paper that was tabled, and there was a statement from Minister Duclos indicating that he had called the president and CEO of Canada Post to reiterate that the protection and preservation of Canadians' right to privacy are of the utmost importance. Following that, Canada Post issued a statement indicating it would conduct a review of its services program to ensure that it lives up to the standards Canadians expect, but that's all I've had.

Ms. Marilyn Gladu: That's good.

I hope they do take action on that. When we looked at the Official Languages Act, we found that the Commissioner of Official Languages needed more enforcement powers as well. I think that's a good point to take forward.

I want to follow up on your discussion about the pandemic and some privacy issues there.

Obviously my employer can't share my vaccination status and my doctor can't share my vaccination status, but during the pandemic, every bar and restaurant had a list of everybody who was there and whether or not they were vaccinated. I thought that was a violation of PIPEDA.

Did you comment about this at all in your recommendations?

Mr. Philippe Dufresne: We made some overall recommendations, mostly towards the public sector. This was my colleague, before my arrival, but certainly there were recommendations in terms of necessity and proportionality, in terms of time limiting and in terms of making sure you were documenting and data minimizing. In the context of our report, we looked at the government's approaches in that sphere, and we applied the necessity of proportionality and made some conclusions there.

Ms. Marilyn Gladu: Were there recommendations of what to do differently in the future?

Mr. Philippe Dufresne: There were some recommendations, certainly. There was one breach in the context of ArriveCAN. We made some recommendations there in terms of stronger safety measures for this type of information and for avoiding errors. This was a situation in which there was an error—people were told they needed to isolate when they didn't—so it was about making sure that you maintain good information and that you get rid of bad information.

We made some recommendations sometimes in terms of the objectives. There were some debates sometimes about the objective in this case. Was it to increase vaccination, was it public health, or was it both? There were some recommendations there, and there were some recommendations in terms of documenting and retaining the information about what other options you considered. They were really in terms of the discipline of that process.

● (1745)

Ms. Marilyn Gladu: Very good. Thank you.

I want to turn my attention to digital technology and Bill C-27.

One concern that's been raised is people worrying about deepfakes, this generative AI that will make anybody look like they're saying or doing things they didn't.

Did you provide any recommendations to the minister or do you have any thoughts on how to fix that?

Mr. Philippe Dufresne: There are three we made specifically on AI that would help that issue. One was mandating privacy impact assessments whenever you have a high-impact system of AI. That would be one. Doing that, as an organization you would need to ask what the risk to privacy is. What is the risk of these types of deepfakes? How are you mitigating that? There are some proposed provisions in the AIDA, the artificial intelligence data act, that would do that as well.

We recommended great transparency for AI decisions. If a decision is made about you, you can ask for an explanation. If you see something that's strange, like a video of you, and you ask that question, you should get that explanation.

We also recommended collaboration among regulators wherever we can. I've just launched, with the Competition Bureau and the CRTC chair, a digital regulators forum, but there are limits on what we can do. We can't collaborate in investigations, for example. I can do that with the FTC in the U.S. and other countries, but I can't do it in Canada. That's a gap that would be easily fixed, and, in my view, it should be fixed.

The Chair: Thank you, Mr. Dufresne.

Thank you, Madam Gladu.

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

Mr. Mike Kelloway (Cape Breton—Canso, Lib.): Thank you, Mr. Chair.

Normally I'm on the fisheries committee, so it's a nice change. Obviously, the work we do here is very, very critical.

I have a couple of questions.

When TikTok was here, they appeared to be concerned about the government banning their app on government devices. Was the decision to do that the right one or the wrong one? Can you unpack that for me?

Mr. Philippe Dufresne: That was a decision that was made by the Government of Canada. The Government of Canada made decisions based on its review, based on the expert assessment of the chief information officer and experts. They made that on the basis of privacy and security considerations. They would be better placed than I would be to discuss this decision.

I have initiated a complaint with my colleagues in Quebec, B.C. and Alberta to look at TikTok's practices in terms of data protection and use, particularly with respect to children. They're different issues. There may be some overlap in certain areas, but they are two separate decisions.

Mr. Mike Kelloway: Where do you think those overlaps are?

Mr. Philippe Dufresne: To the extent that they're privacy concerns from the government in making its decision, and there were some privacy concerns stated, there may be some overlaps there. I'm not involved in that assessment from the government side.

My focus in the investigation will be to look at the data practices, the consent for appropriate purposes, with a particular focus on children and youth, because they are the majority of the users.

Mr. Mike Kelloway: They're the vulnerable users.

Mr. Maguire, do you have any thoughts on that?

Mr. Michael Maguire (Director, Personal Information Protection and Electronic Documents Act, Compliance Directorate, Offices of the Information and Privacy Commissioners of Canada): I don't think I would add anything, no.

Mr. Mike Kelloway: Thanks for that.

I know this is going to surprise both of you, but I'm not a techie. I use Facebook, I use TikTok and I use Twitter.

For parents at home or people at home, Mr. Villemure talked about whether the toothpaste was out of the container, as it were. Is there any advice you can give people who are watching this, or may watch it later, on how to best protect their privacy, based on the work you've done?

Mr. Philippe Dufresne: I would say a few things. One is that we've issued a declaration with my federal, provincial and territorial colleagues called “Putting best interests of young people at the forefront of privacy and access to personal information”. It's available on our website. We give a number of recommendations and expectations for organizations about making sure that they're protecting children and the best interests of the child and that they're treating their information appropriately.

In terms of what people should do—and that's something we've said in our data-scraping statement with my international colleagues—ask yourself if you are comfortable sharing this much information. Do you know enough about the settings and the protections that are there? Is this something you want to potentially see forever?

In Bill C-27, there's a new proposed section to dispose of information, especially for minors. That's good, but whenever you're putting a picture of your children online, ask yourself if you want to take the risk. Have you put the privacy settings in a strong enough way? Are you sharing this with the whole world? If you don't understand enough about what the organization is doing and you find its privacy policy to be complex, I always encourage everyone to ask the organization.

Ask for more information. When stores ask for your birthday, ask them why they want to know your birthday when you're buying jewellery or any kind of item. Why do they need that information?

It's getting that reflex of not just saying, “Yes, sure, I'll give it to you.”

● (1750)

Mr. Mike Kelloway: Mr. Chair, how much time do I have?

The Chair: You have 50 seconds.

Mr. Mike Kelloway: I think you touched upon this to some degree, but can you speak in a bit more detail in the time we have about the collaboration and coordination that go on with the other regulatory bodies, particularly law enforcement?

Mr. Philippe Dufresne: We have exchanges with other regulators, those being the Competition Bureau and the CRTC. We've launched this new digital regulators forum, and the goal is to talk about areas of common interest with privacy components and law enforcement. We have exchanges with the RCMP to discuss issues of new technology and provide our input. We have a government advisory section, so we're always engaged in these types of—

Mr. Mike Kelloway: Are local police involved in that? The RCMP is, yes, but do we deal with the other municipal—

Mr. Philippe Dufresne: I think it's been mostly with the RCMP, but perhaps....

Mr. Michael Maguire: Local police fall under provincial jurisdiction.

Mr. Mike Kelloway: Thank you.

The Chair: Thank you, Mr. Kelloway.

It's always solid, Mr. Dufresne. I appreciate that.

That concludes our first hour. What I would like to do is roll right into the next hour and give Mr. Dufresne a second to get his notes together.

I want to make the committee aware that I had a request from TikTok to extend by a week the requirement to provide us with written responses to the written questions. If the committee recalls, it was supposed to be this Friday. They've asked to have until next Friday.

With the committee's consent, I'd like to give them that extension so that we get the answers we need. Is that okay?

Some hon. members: Agreed.

The Chair: We had a lot of crosstalk about TikTok, so we're going to move into our second hour, which is our social media study focused on TikTok.

Mr. Dufresne, if you'd like to address the committee for five minutes, I'd appreciate that. We'll then get into questioning.

Thank you. Go ahead.

Mr. Philippe Dufresne: Thank you, Mr. Chair.

I'm pleased to now turn to this part of the discussion. I thank the committee for its interest in the ways that social media platforms such as TikTok harvest, handle and share personal information.

The online world brings with it a host of possibilities for innovation and connection, but it also carries potential for significant harm, especially for young people.

As you know, my office, along with our counterparts in Quebec, British Columbia and Alberta, launched an investigation into TikTok in February. We are examining whether TikTok's practices comply with Canadian privacy legislation, and in particular whether it obtains valid and meaningful consent for the collection, use and disclosure of personal information.

We are also looking at whether a reasonable person would consider the purposes for which it handles personal information, in particular children's information, to be appropriate in the circumstances.

[*Translation*]

This matter is a high priority for my office, especially given the importance of protecting the fundamental right to privacy of young people, who represent a notable proportion of TikTok users. As a result of the ongoing investigation, there are limits to my ability to speak publicly about the company's practices at the moment.

For that reason, I will focus my remarks today on the privacy principles that underpin my office's approach to the digital world from the perspective of the privacy rights of children.

Growing up in the digital age presents significant new challenges for the privacy of young people. As children and youth embrace new technologies and experience much of their lives online, we need strong safeguards to protect their personal information, and how it may be collected, used and disclosed. Increasingly, their information is being used to create personalized content and advertising profiles that are ultimately aimed at influencing their behaviours.

[*English*]

Children have a right to be children, even in the digital world. As UNICEF notes in its policy guidance on artificial intelligence for children, young people are affected by digital technologies to a greater extent than adults. Young people are also less able to understand and appreciate the long-term implications of consenting to their data collection. Privacy laws should recognize the rights of the child and the right to be a child. This means interpreting the privacy provisions in the legislation in a way that is consistent with the best interests of the child.

I'm encouraged by statements from the Minister of Innovation, Science and Industry indicating that there is a desire to strengthen children's privacy rights in Bill C-27, the Digital Charter Implementation Act, 2022. My office has recommended that the preamble of the modernized federal privacy law should recognize that the processing of personal data should respect children's privacy and the best interests of the child. I believe that this would encourage organizations to build privacy for children into their products and services by design and by default. I was pleased to hear the minister signalling his agreement with that recommendation.

● (1755)

[*Translation*]

The law must have strong safeguards to protect children's information from unauthorized access, and reflect greater consideration of the appropriateness of collecting, using and disclosing their information.

Earlier this month, my provincial and territorial colleagues and I adopted a resolution calling on organizations in the private and public sectors to put the best interests of young people first by, among other things, providing privacy tools and consent mechanisms that are appropriate for young people and their maturity level; rejecting the kind of deceptive practices that influence young people to make poor privacy decisions or to engage in harmful behaviours; and allowing for the deletion and de-indexing of information that was collected when users were children.

I am happy to see this was included in Bill C-27.

[*English*]

In closing, it's critical that government and organizations take action to ensure that young people can benefit from technology and be active online without the risk of being targeted, manipulated or harmed as a result. I expect that the findings from our investigation into TikTok will be informative not just for that company but also for other organizations that collect and handle children's sensitive personal information.

I also look forward to seeing Bill C-27 progress through the legislative process in a way that will provide children and minors with the privacy protections that they need in this increasingly digital world.

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

The Chair: Thank you, Mr. Dufresne.

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

Mr. Michael Barrett: Thanks, Chair.

Thanks very much for continuing your appearance with the committee.

Can you give us more detail about the scope of the investigation and the complaint that you've initiated against TikTok, or concerning the issue of TikTok?

Mr. Philippe Dufresne: Sure. When we announced the investigation on February 23, 2023, we indicated that this was initiated in the wake of now settled class action lawsuits in the U.S. and Canada, as well as numerous media reports related to TikTok's collection, use and disclosure of personal information. We indicated that the four privacy regulators will examine whether the organization's practices are in compliance with Canadian privacy legislation and, in particular, whether valid and meaningful consent is being obtained for the collection, use and disclosure of personal information.

The investigation will also determine if the company is meeting its transparency obligations, particularly when collecting personal information from its users. We added that an important proportion of TikTok users are younger users, and that given the importance of protecting children's privacy, the joint investigation will have a particular focus on TikTok's privacy practices as they relate to younger users, including whether the company obtained valid and meaningful consent for these users for the collection, use and disclosure of their personal information.

In the course of the investigation, we have now added an element of reviewing whether this was done for appropriate purposes, which is another element of the act. That's now been added to those elements under review.

Mr. Michael Barrett: Has TikTok been co-operating with your investigation and the inquiries you made?

Mr. Philippe Dufresne: I'll look to Mr. Maguire. My sense is that—

Mr. Michael Maguire: They have been co-operative.

Mr. Michael Barrett: Does your investigation extend, or have any reach, to their parent company, ByteDance?

Mr. Michael Maguire: The investigation involves ByteDance as the owner of TikTok.

Mr. Michael Barrett: The National Intelligence Law was passed by the CCP, the Chinese Communist Party, in 2017. It requires any organization to assist or co-operate with state intelligence work. That's on top of a 2014 law that says relevant organizations may not refuse to collect evidence for an investigation.

Does that cause concern? What assurances are you able to extract from ByteDance that their responsibilities to the Communist dictatorship in Beijing won't supersede privacy requirements here in Canada?

● (1800)

Mr. Philippe Dufresne: Again, we are focusing on specifically data practices with respect to children's information. We're looking at the safeguards, tools and rules.

There is a provision under PIPEDA that talks about an organization being responsible for information in its “custody, including information that has been transferred to a third party for processing.” They “shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.”

However, the focus of the investigation here is very much in terms of what ByteDance is doing with the information of children.

Mr. Michael Barrett: Did you watch the testimony from the representatives from TikTok at this committee last week?

Mr. Philippe Dufresne: I reviewed the transcript.

Mr. Michael Barrett: Is all the information provided in their testimony consistent with the evidence you reviewed as part of the complaint you have undertaken?

Mr. Philippe Dufresne: I have not looked at it from that standpoint.

The investigation is ongoing. We have not made our findings and we have not drawn our conclusions, so I wouldn't be in a position to draw conclusions on this point, at this stage.

Mr. Michael Barrett: Do you know where Canadian user information for TikTok is stored? Do you know where those servers are?

Mr. Philippe Dufresne: I think, in the testimony of the TikTok witnesses, they mentioned Singapore, if I remember the transcript I saw.

Mr. Michael Maguire: I'll simply add that in the context of an investigation, we wouldn't be able to share information that's been provided to us in the investigation at this time. We have the ability to publish a report of findings, and when we have completed our investigation, we would share further information we obtained during it.

Mr. Michael Barrett: What type of recommendations would you make to Canadians following a report into a platform like this? Can you take us through what your recommendations might look like? You've talked about your recommendations to the entity, but what about to the Canadian public?

It's one thing for you to tell Acme Co., “You ought to do this”, but what about telling the Canadian public what they ought to be doing when interacting with a platform about which you may or may not have identified concerns?

The Chair: You have to keep it tight. You have 30 seconds.

Mr. Philippe Dufresne: Sure.

I'll give you an example of what we did with Home Depot. When we made that investigation public, we talked about the recommendations we made to Home Depot, but in doing that—I don't recall whether it was in the report of findings itself, or in my statement—we gave advice to Canadians.

In saying that, ultimately I don't want it to be delegated to Canadians to protect their privacy: The obligation is on organizations. However, there are good tools and practices, and we would certainly take that opportunity.

Mr. Michael Barrett: Would you go so far as to tell Canadians not to use a service or not to use an app, or not to provide their information to a business?

The Chair: Very quickly....

Mr. Philippe Dufresne: I don't want to speculate as to what we would say, but we would consider appropriate advice to Canadians in a circumstance.

Mr. Michael Barrett: Thanks for your answers.

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

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

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

Thank you to the witnesses for appearing today on double shift with two different issues. We really appreciate it.

I want to pick up on something you said with respect to your study and report based on children and TikTok.

How much of a distinction is there between privacy rights specifically for children and for the general public at large? Is there a significant overlap, or are there extra issues we deal with for children?

Mr. Philippe Dufresne: There are extra issues, in the sense that we will generally consider minors' information or children's information to be "sensitive information". That brings with it greater obligations in terms of care and in terms of methods of consent.

We've issued guidance under current law about obtaining meaningful consent. We are expecting organizations to make it user-friendly and so on, but specifically with respect to children, there are circumstances in which they won't be able to give that consent. They may need a parent to do that if they're below a certain age. In our current guidance, although certain provinces might take different views, for us, if they're under13 years old, there's almost a presumption that you need that parental consent.

It certainly has to be considered in how you look at information. They will have different needs. They will have greater vulnerabilities. That is something that's recognized in the European legislation. It's proposed to be recognized in Bill C-27, which I certainly hope will happen.

● (1805)

Ms. Iqra Khalid: You talked about meaningful consent. What does that look like in the context of social media platforms that have so much access to Canadians' information?

Mr. Philippe Dufresne: Again, in terms of meaningful consent, Bill C-27 would make it stronger in terms of explicitly saying that this has to be provided in information that the person can understand. That's what we look at. This is very complex information. How are you giving those notices? Are you giving a notice that only an expert will understand?

Even if you're an expert, you may be reviewing this at the end of the day. You may be tired. You may be bombarded with so many things. Every time you go on a website, you get a cookie page or whatnot. We provide a number of tips in that guidance: Make it user-friendly. Make it not just a one-time thing. Make sure that you sometimes provide follow-ups. Make it as understandable as possible. In the context of children, make it appropriate to the child. Maybe there are opportunities for video or other ways.

The goal is to provide the information so that individuals can understand what's going on and to bring that same innovation.... We often talk about innovation requiring data, and that's true, but let's use innovation to protect data. That would assist in terms of the consent and the explainability.

Ms. Iqra Khalid: How does that protection of data play out when we see that a company like TikTok is storing data in the U.S., in Singapore, in Malaysia and not in Canada? How do we control the servers or the access to Canadian data when it's physically not present in Canada?

Mr. Philippe Dufresne: Right. Well, the law will still apply if Canadians are affected. A number of factors will give us jurisdiction, even if the information itself may be stored elsewhere. We look at those factors, those links, and then we apply the law to the organization and to the treatment of the information at issue.

Ms. Iqra Khalid: Thank you.

When we had TikTok representatives here with us, David Lieber, who appeared at the last meeting, said the following:

> We also have a biannual transparency report where we disclose [a] number of government requests that we receive from governments throughout the world....if we did receive a request from the Chinese government, we would certainly disclose it in our transparency report.

Have you looked at these transparency reports? What kinds of details do they provide? Are they actually transparent?

Mr. Philippe Dufresne: In preparing for this appearance, I was briefed on these types of reports. I think the question to be considered is about the extent of it. If you're pointing to a report to say that this report will give transparency, I would ask what the report is about. What will it report on? Will it report only on Canadian government requests? Will it report on governments all over the world? That's an important element to make sure of.

Ms. Iqra Khalid: Especially with data not being stored physically in Canada, if there's a request made by X, Y, Z state or country to say, "Hey, TikTok, can you give us all the data on every 16-year-old girl who likes MAC lipstick?", should TikTok have a duty to report to Canadian authorities the request for information by a country that is not Canada?

Mr. Philippe Dufresne: This is not something that we've investigated or turned our minds to. Generally, if we look at a matter on the protection of information, we'll look at the safeguards. We'll look at what the risks are. We'll look at what measures you're putting in place to protect that information. Based on that, we'll make our recommendations and our findings.

Ms. Iqra Khalid: Do you find that companies like TikTok and other social media platforms would heed some of your recommendations? How do you anticipate that some of your recommendations would be applied within Canada in terms of privacy?

Mr. Philippe Dufresne: This is where the order-making power is an important element. Right now, we would make recommendations. It's up to them to decide if they're going to follow up. If there's order-making power, that can be enforced.

● (1810)

[*Translation*]

The Chair: Thank you, Ms. Khalid.

It's now over to Mr. Villemure for six minutes.

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

Mr. Dufresne, how would you describe the platforms' appetite for protecting privacy?

Mr. Philippe Dufresne: What I can tell you is that the platforms attend privacy conferences. They are very involved, very aware and very interested when it comes to privacy issues.

My office examines what the platforms do and how they use the information. That's what our recommendations are based on. For example, we give platforms recommendations on data scraping, so the practice of collecting large amounts of data on the web. We let the platforms know that we expect more of them. We expect them to be more proactive, and to treat data scraping as though it were an invasion of privacy and to protect and handle the information accordingly. We are engaging with them. They've sent us feedback on our position, and we are engaged in a discussion.

As I mentioned earlier, we are involved in a court challenge against Facebook related to the use of information by Cambridge Analytica. We are also conducting investigations into ChatGPT and TikTok. The process exists. Intentions and statements aren't what interest us. What we care about is real results for Canadians.

Mr. René Villemure: In other words, you care about everything that's said and done.

Would you say that, every time you manage to make some headway on privacy, the platforms look for ways around it or ways to go further in order to protect their business, which is basically selling people's data?

Mr. Philippe Dufresne: I think we have to be aware that there is often an economic incentive to use information. It's normal, it's part of the economic system. States and regulatory bodies must therefore be able to create incentives in the other direction to protect information. I see two kinds of incentives. First, there's a positive incentive, which recognizes good behaviour and gives reputation-related rewards; but you also need a negative incentive, which uses legal constraint. We need laws that will tell these platforms and organizations that they have a proactive obligation to publish their privacy plan, that they have a proactive obligation to conduct audits, that they have a proactive obligation to minimize data use and explain it properly. If they don't, there can be audits, investigations, orders and fines. I think all this is necessary to have proper regulation.

Mr. René Villemure: Is your power a sufficient deterrent to force platforms to follow your recommendations? We mentioned the power to issue orders, but do you lack other tools?

Mr. Philippe Dufresne: At the moment, I lack the power to issue orders and the ability to impose administrative monetary penalties. If an organization is raking in millions or tens of millions of dollars using data and there are no monetary penalties when a breach occurs, going in that direction becomes tempting. This must be avoided.

Mr. René Villemure: For companies with billions of dollars in sales, I don't know what a deterrent fine would be.

We've heard about the 345-million euro fine imposed on TikTok in Europe, for multiple infringements. However, how effective is such a fine when the company has multi-billion dollar sales?

Mr. Philippe Dufresne: That's why the European model, which is the General Data Protection Regulation, the model in Quebec, which is Bill 25, and the model proposed in Bill C-27 provide that it's going to be a maximum amount of $10 million, for example, or 3% of sales. I think that addresses the issue you raised.

If a company has significant sales, $10 million isn't a lot; setting a percentage addresses that.

Mr. René Villemure: According to the European community, establishing a percentage works well.

What do you think about TikTok being banned in several countries around the world, including some European communities?

Mr. Philippe Dufresne: I think institutions and regulatory authorities like ours need to do their job, investigate complaints and verify compliance. If there is no compliance, they should issue orders or make recommendations. I also believe that governments have a responsibility for national security and the security of public servants' information. That's what the Government of Canada has done in this case by talking about the work tools of public servants, tools that deal with very sensitive information. I think this is part of the responsibility of states.

Mr. René Villemure: You talk about national security. However, we associate TikTok with a hobby. We don't think for a moment that it could have an impact on national security when, in reality, it does.

Last week, a TikTok representative was asked if TikTok sold data to the parent company. He replied in the negative, but, all of a sudden, he somehow dropped the words “We share.” In other words, TikTok shares data.

What do you think of this data sharing?

● (1815)

Mr. Philippe Dufresne: Data sharing, whether paid or unpaid, is targeted. There are restrictions on what can be done in the way of data collection, disclosure and use.

Mr. René Villemure: There is a particular concern that they share data with the parent company, which is still recognized as part of the Chinese communist regime.

Mr. Philippe Dufresne: In my opinion, this is part of the context that needs to be considered. In the case of sharing, one must check whether it is appropriate, whether it respects legal limits and whether it gives rise to security concerns.

There are various players in the system. Now, it is useful and good that they can publicize, in an appropriate way, such conclusions. This underlines that there are institutions, that they function and do their work.

Mr. René Villemure: Thank you very much.

The Chair: Thank you, Mr. Dufresne.

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

Mr. Alexandre Boulerice: Thank you very much, Mr. Chair.

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

I'll take a brief step back in time. In the last century, when people bought a newspaper in the morning, they felt they were buying a product that gave them news, an account of what was happening in their society. But then someone thought about it and said that the newspaper was actually selling the reader to the person who was buying advertising in the paper. The buyer wasn't who we thought. In those days, a company that owned a lingerie store, for example, and bought advertising in the newspaper generally had no idea who its customers were or even who the newspaper's readers were.

Today, however, with social media, the dynamic is completely different. Indeed, people almost voluntarily provide their personal information to large conglomerates that sell or share this information in order to make huge profits. In other words, citizens provide information free of charge, enabling these large companies to target advertising precisely to their wants, desires and needs. At the same time, this enables large companies, large conglomerates, to reap considerable profits.

You spoke earlier of a consumer or citizen reflex. Do you get the impression that most people around us understand that they are selling themselves for free to the Web giants and social media?

Mr. Philippe Dufresne: There's an expression that says if it's free, you're the product. That's exactly what you're describing. I think we need to be aware of this. When we buy a product and they ask us our date of birth and tell us it's because they're going to give us a discount on our birthday, that's exactly what's happening. We're given a small discount and that information is used.

It's important to make people aware of this phenomenon so they know, even if they feel it's free, that in some cases they're giving up a fundamental part of their identity, their personality.

We need to be aware of this fact and avoid seeing it solely as an advantage. Indeed, one should not simply sell or trade one's privacy. Even if consent is given correctly, we must always be aware that it is a fundamental part of our individuality. That's an important point.

Mr. Alexandre Boulerice: Thank you, Mr. Dufresne.

In one of his sets, which I won't redo here, Louis-José Houde says that just because he buys a spatula doesn't mean we'll have access to his cell phone.

On a more serious note, in 2019 you did an investigation into Facebook, which is now called Meta. The report included four major findings, which were quite disturbing, namely that Facebook failed to obtain valid consent from not only users, but also from those users' friends or contacts. In addition, measures to protect users' personal information were inadequate. These four findings are quite worrying, given the popularity of this platform.

Since you carried out this investigation and came to these four conclusions, what exactly has happened?

● (1820)

Mr. Philippe Dufresne: The law doesn't give us the power to issue orders, as we've discussed. What the law does allow us to do is to go to the Federal Court, re-argue the case before the Federal Court of Appeal and ask them to issue the order that we recommend. So that's what's been done.

The Federal Court dismissed our application after hearing it and concluded that the claim had not been established. We then appealed on the two fundamental issues you identified, namely consent—there are several levels of consent to protect data—and security measures.

I announced this appeal saying that it dealt with issues important to Canadians. We were not satisfied with the Federal Court's decision, and we wanted the Federal Court of Appeal to be able to rule on this issue. We are waiting to argue before the Federal Court of Appeal and we will then get a decision.

Mr. Alexandre Boulerice: Based on what you understand and what you know, do you believe that Facebook's practices, or Meta's, represent the exception in the world of social media? Are they more representative of the behaviour of these large companies?

Mr. Philippe Dufresne: I hesitate to generalize, especially when it's a specific case that's before the courts. However, I can say that when we draw conclusions, if there is a case for broader conclusions, we do so.

I expect social media to be aware of the decisions we make. If it's a specific case, I always invite organizations to review their practices and, if they have similar practices and we've found them to be a violation, it's up to them to correct them.

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

[*English*]

Before we proceed to the next round, I have had a request. I want you to consider this request. I'm not asking for consideration now, but I will ask at the end of the meeting.

As I mentioned at the onset of this particular round, there was some discussion about TikTok in the last hour. The request is to have some of that information extracted and placed into this report, which is relevant to our study on TikTok.

I see that Mr. Barrett is not here. He has stepped out for a second. That's why I want to give you a bit of a notice to consider this.

Ms. Gladu, you have five minutes. Go ahead, please.

Ms. Marilyn Gladu: Thank you, Chair, and certainly I think it would be a good idea to incorporate that data.

I want to continue on the questions about Meta, because the government made 2,859 requests to Meta between January and June of 2022 to restrict access to content. Do you know if any of those requests were related to concerns about privacy or about where the data might be going?

Mr. Philippe Dufresne: I'm not aware of that. I don't have information on that, unfortunately.

Ms. Marilyn Gladu: Very well. Let me go on to TikTok, then.

One of the concerns is that ByteDance might be sharing data, so you're looking into the situation. How would you verify what they say? How are they going to show that they're actually doing the protections that are required by law?

Mr. Philippe Dufresne: There are a number of tools in the act in terms of site visits or in terms of requests for documentation. We have a technical lab at the OPC, so we're looking at technical tools to be able to do the investigations and obtain the information we need.

I don't know if Mr. Maguire has anything to add in terms of general investigative tools.

Mr. Michael Maguire: We also have the ability to interview, including under oath, as well as to visit the site to require the production of information or documents or things. We have the ability not only to ask questions but also to ask that those be sworn and, finally, to verify through testing, either remotely or on site.

● (1825)

Ms. Marilyn Gladu: That's excellent.

What about the concern with cyber-breaches? I know you indicated in the earlier hour that there have been fewer reported cyber-breaches within the government, but there is a suspicion that perhaps there is under-reporting. What about breaches of people's personal data from these various social media platforms? What can you tell us about the situation there?

Mr. Philippe Dufresne: In our annual report, we've provided statistics for both the public sector and the private sector.

In the context of the public sector, the overall comment was that we find the level of reporting low. It feels as though it must be higher than that in reality, so we're curious about that and we're flagging it.

In terms of the private sector, we've seen increases as well in terms of breaches. We have received notifications of those breaches and we are in contact with organizations when they occur. This is something that is a big focus because of the privacy harm this could do to Canadians.

Michael, do you have some statistics?

Mr. Michael Maguire: I don't have statistics, but I would add that what we have seen are examples of scraping of users' data from social media in cases like those of Clearview AI and Profile Technology before that. We found those to be unauthorized scrapings.

With our 11 international counterparts from six continents, we issued a joint statement on data scraping and directed that to social media companies, asking them to discuss how they comply with the expectations we identified in that statement. We continue to engage with those social media companies to get a sense of the best practices and potentially to make recommendations to improve protection against scraping of information off their platforms.

Ms. Marilyn Gladu: That's excellent.

In terms of the complaints you received, you said they were up 37% overall. What percentage of those are related to social media platforms, and has that percentage or distribution changed over time?

Mr. Philippe Dufresne: I'll ask my colleague for the specific statistics.

We have them in the annex of the report, listed by department, in terms of the public sector. As well, we are listing, in terms of—

Ms. Marilyn Gladu: It's okay if you want to just make sure you send the reference to that to the clerk, and it can be distributed.

I have a final question. I'm running out of time.

What would you recommend this committee recommend to the government to do to better protect the privacy of Canadians?

The Chair: Could that be in 13 seconds?

Mr. Philippe Dufresne: As legislators you can do a lot to protect the privacy of Canadians by amending public sector and private sector privacy legislation. Those are really ultimately the first tools we use to do our job.

The Chair: Thank you, Mr. Dufresne.

Ms. Damoff, you have five minutes. Go ahead, please.

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

Thank you for being here.

I remember someone who had a marketing company saying a number of years ago that people give a lot more of their personal information when they're doing it online versus when they actually talk face to face with a person. That's certainly true on social media too, when you think about the things you're sharing.

Do you think the government should be investing more money in educating Canadians about digital literacy and the privacy concerns that you've expressed? I don't think people think about these things.

Mr. Philippe Dufresne: I do. I think we should do more at all levels.

This is something I would want my office to do more of. We have a promotion mandate, and we're looking at it and thinking about how we can do that, particularly with respect to children. That was a big part of our internal discussions. I'll be consulting stakeholders as well. I am having lots of discussions with industry and governments and academia about how we can reach out and do more for Canadians to help them understand about their privacy, particularly but not only when it comes to young children.

This resolution that we issued this month with our provincial and territorial counterparts is an effort we have made to state some of the expectations on how you need to protect children's information and how you should do that.

This is a collective effort for government, absolutely, and for schools and teachers.

Ms. Pam Damoff: I think it should be children in particular, because they're more vulnerable, but I don't think parents think about that when they let their kids go onto social media platforms.

I know we've talked a lot about TikTok today and about kids being vulnerable. Is it just TikTok, or is it all social media platforms, and is it a problem for kids because they tend to be the predominant users of TikTok?

● (1830)

Mr. Philippe Dufresne: It's a problem for kids because of their greater vulnerability. We've made a number of recommendations in terms of making sure that we're not using these behavioural techniques of nudging. We shouldn't be nudging individuals generally, but certainly not children, into making bad decisions and making bad privacy decisions. There needs to be work on that.

There have been reports on social media being addictive and being addictive for children generally. Sometimes the business model is to try to encourage them to stay longer, because that's what generates more revenues. That has to be taken into consideration with children who have been online more and more during the pandemic, and since then with school. I've seen it and parents have seen it.

We need to adjust to this new reality as parents, children and society as a whole, so that there's a greater awareness of what this means and what their rights are.

Bill C-27 proposes a right to disposal. That's informing.... When I say that children have a right to be children, that's what I'm alluding to. Children do things online. If it stays online forever, then they're treated as adults right from when they're teenagers. It stays forever, and it could be used against them for jobs and so on and so forth.

We need to deal with this. Bill C-27 will deal with it to some extent, but we certainly need to build greater awareness of it as we are living more and more in a digital world. It brings innovation and it brings great things, but we need to be well equipped to deal with it and we need to learn about it. I would hope to see mandatory training in schools early on, so that individuals can get the tools early on.

We'll get these reflexes. We're going to ask questions. We're going to ask why they need this information. We're going to learn to see what a good privacy policy is, and if it's not, we're going to learn how to complain about it so that it could become a good privacy policy in the future.

That way, we're creating ambassadors for privacy everywhere.

Ms. Pam Damoff: I have only a minute or less left.

Privacy policies come up as very long and as very much stated in legalese. Is there a way that those could be simplified for people before they say “accept”?

Mr. Philippe Dufresne: Absolutely. They need to be simplified. They need to be shorter and more concise, and they need to get to the heart of it.

Sometimes you have a very long-drawn-out legalistic policy that doesn't really communicate very important things that could be done more briefly. You agree to this and you agreed to sharing it with third parties, including parties outside of Canada. If you agree to this policy, they can make inferences about you and draw conclusions that go beyond what you're giving them. You need to know that. They can guess your age. They can guess a number of things about you.

It's finding that balance in terms of content and conciseness.

The Chair: Thank you, Ms. Damoff.

[*Translation*]

Our next speaker is Mr. Blanchette-Joncas, whom we welcome to the committee.

You have two and a half minutes, Mr. Blanchette-Joncas.

Mr. Maxime Blanchette-Joncas (Rimouski-Neigette—Témiscouata—Les Basques, BQ): Thank you very much, Mr. Chair.

Good evening to my colleagues and the witnesses who are with us tonight.

My question is quite simple, but the answer can be quite complex.

Can you tell us whether you think a revision of the law is necessary, and explain why?

Mr. Philippe Dufresne: Yes, a revision of the two laws is necessary. One is under way for the law in the private sector. This is Bill C-27. This also includes a specific component for artificial intelligence.

A revision is necessary because the law is 20 years old. It's older than social media. We're still applying it, the principles are there, but technology is advancing rapidly. In my opinion, this calls for stronger proactive obligations, for example. We need to force organizations to make basic assessments that they have to disclose to our office; we also need to impose greater transparency, particularly when it comes to artificial intelligence.

The law governing the public sector, on the other hand, is even older. It dates back 40 years. It needs to be modernized and strengthened, because when it was passed, it was really at a time when the impact of data was not what it is today.

Mr. Maxime Blanchette-Joncas: That's right. As you mention, social media didn't even exist when this law was passed.

Can you explain concretely the consequences of having a law that is outdated and doesn't reflect today's reality, in 2023?

● (1835)

Mr. Philippe Dufresne: Fortunately, the law is based on principles. So we're able to apply those principles to organizations that use and disclose data. That's what allows us to investigate TikTok and ChatGPT.

That said, there are shortcomings: we don't have the power to issue orders or fines.

In the case of organizations making huge profits from data, there is a shortcoming. It may not have been an issue before because companies weren't making so much money from data, but, now, they are.

So there have to be fines. We need to be more proactive. We need greater transparency. Explaining decisions made by algorithms, by artificial intelligence, obviously wasn't a problem. We can regulate this with principles, but there are certain things that become a little more technical. I think that, when it comes to artificial intelligence and algorithmic decisions, our requirements need to be broad enough that they still apply five years from now, ten years from now, to ChatGPT's successors. These requirements must be reinforced.

Mr. Maxime Blanchette-Joncas: Thank you very much.

The Chair: Thank you, Mr. Blanchette-Joncas and Mr. Dufresne.

For the last intervention, the floor goes to Mr. Boulerice for two and a half minutes.

Mr. Alexandre Boulerice: Thank you.

Mr. Dufresne, in your presentation, you talked a lot about protecting children and teenagers. I'm wondering how we can ensure that the age required to participate in social media is respected. For example, I think you have to be 13 to have a TikTok account and 14 in the case of Facebook.

That said, we all know that there are plenty of youngsters who are perfectly capable of getting around these rules and creating an account anyway.

What's the responsibility of companies and the government to make sure the age requirement is respected? Otherwise, it becomes pretty easy to sign up for social media.

Mr. Philippe Dufresne: Indeed.

This raises the whole question of online age verification and techniques for determining whether a person is underage or not. This will be important in the context of Bill C-27, which explicitly grants rights and treats information differently. It's an issue we're looking at, in the privacy field. There's a lot of discussion about it. In fact, the Information Commissioner's Office of the U.K. has issued guidelines on verification tools.

What we're saying, at the Office of the Privacy Commissioner, is that these tools need to be appropriate and not ask for too much personal information. Age verification needs to be managed, but we don't necessarily want to ask for too much personal information to do that. That said, there are ways of doing it and technologies to do it. It's another area where we need to be creative.

Also, it has to be context-appropriate. Some sites may be higher-risk and will require tighter verification. We can think of gambling or pornography sites, for example. Some sites may be less sensitive. Others may be aimed specifically at children. There may be a presumption.

I think this will be part of the implementation of this law. My office will have a role to play in this as it can issue guidelines.

In addition, the bill also provides for the creation of codes of practice and certification programs.

This will encourage organizations to adhere to a series of rules. If they respect them, it will have an effect on the complaints process, which will be beneficial for these organizations. So it will be one more tool. I suspect that the Office of the Privacy Commissioner will be able to work on it, precisely to give these details.

The Office of the Privacy Commissioner also has an advisory mandate. Companies, especially small and medium-sized enterprises, can contact us for answers to specific questions. We're here to help them with questions like these, especially those of a more technical nature.

The Chair: Very well.

Thank you, Mr. Dufresne and Mr. Boulerice.

[*English*]

Before we go, first of all, I want to thank you, Mr. Dufresne, for being here today. I know a couple of hours is a long time. You were solid, as always.

Mr. Maguire, thank you for being here. You were solid in support.

On behalf of Canadians, I want to thank you for your service to our nation.

My understanding is—I caught up with Mr. Barrett—that there is consent to extract the first hour of TikTok information to put into this study, so we will do that and we will make sure that the analysts do that.

That's it for today.

I want to thank everyone. Thank you to our clerk, our analysts and our technicians.

The meeting is adjourned.