HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

45th PARLIAMENT, 1st SESSION

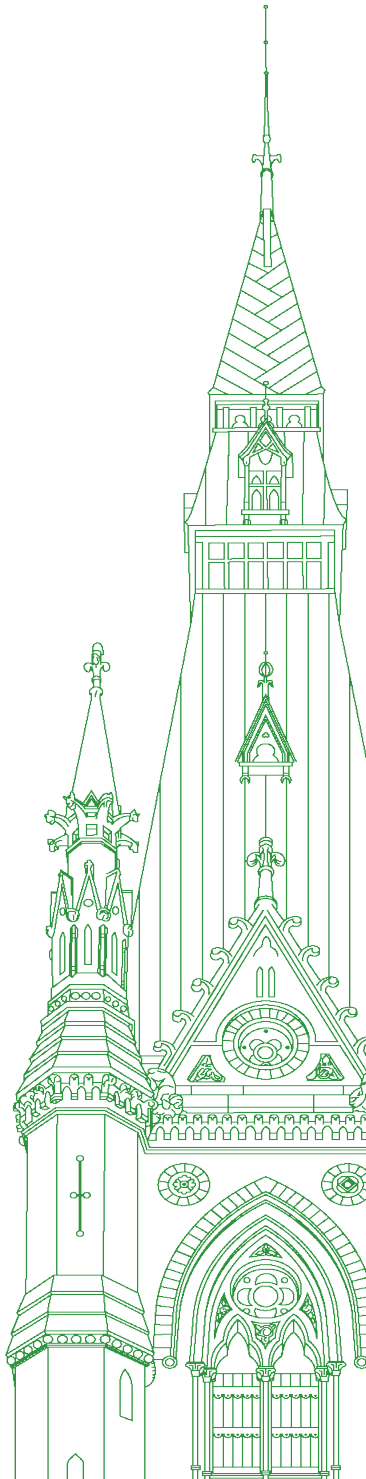
Standing Committee on Industry and Technology

EVIDENCE

NUMBER 021

PUBLIC PART ONLY - PARTIE PUBLIQUE SEULEMENT

Monday, January 26, 2026



Chair: Ben Carr

Standing Committee on Industry and Technology

Monday, January 26, 2026

● (1535)

[*Translation*]

The Chair (Ben Carr (Winnipeg South Centre, Lib.)): Good morning, everyone.

[*English*]

Welcome back to Ottawa. I hope everybody enjoyed a set of quality moments with friends and family over the course of the holiday. We're certainly being greeted with some winter weather, although I want to note for the record, for all those from Ontario and other parts of the country complaining, that my partner sent me a note yesterday to show that in Winnipeg it was -51°C with the wind. Unless where you come from is worse than that, thanks for your understanding about how we Manitobans feel.

This is a retreat, is it not, Ted?

Ted Falk (Provencher, CPC): It's a retreat.

The Chair: Colleagues, for our first hour today, we have something a little bit out of the ordinary in the course of our normal affairs but is ordinary within the affairs of Parliament as a whole. I received a letter from the chair of the finance committee to ask for our assistance in reducing the load they have to undertake in the evaluation of the BIA, the budget implementation act. She has done this with many other committees. It's common practice in order to have efficiency within the process at committee.

Pursuant to that standing order, today we have an evaluation of an act to implement certain provisions of the budget that are relevant to our committee—in particular, clauses 389 to 398, division 23; clauses 589 to 591, division 39; and clauses 597 and 598, division 43.

We will have two guests with us today. Following that, Minister Joly and her officials will be here next week. That was the ask from the finance committee. We are fulfilling that in today's meeting and in Monday's meeting, assuming the schedule goes according to plan.

Joining us today are Philippe Dufresne, Canada's Privacy Commissioner, and Marc Chénier, deputy commissioner and senior general counsel. They will speak to their responsibilities within the BIA and why they're here today. Then there will be an opportunity, as always, for members to speak.

I am going to hold us to time today. We'll end this at exactly the one-hour mark. We have things to get to in the form of a draft report and a couple of other items of business.

With that, Monsieur Dufresne, I will pass the mic to you. The floor is yours for up to five minutes, sir.

[*Translation*]

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

Thank you for the invitation to appear today to share my views on the privacy impacts of division 23 of part 5 of Bill C-15, budget 2025 implementation act, no. 1.

Privacy is an important, topical issue in Canada. As more and more personal data is collected, used and shared, protecting it becomes increasingly important to Canadians and Canadian organizations.

[*English*]

In the past two years, we've seen many examples of how Canadian privacy law can address major issues that cause serious and long-lasting harms to individuals—for example, protecting against the non-consensual sharing of intimate images in my investigation into Aylo, which operates Pornhub and other pornographic websites, and addressing the 23andMe breach, which impacted the highly sensitive personal information of seven million customers, including more than 300,000 Canadians.

My recent investigation with my provincial counterparts into TikTok, meanwhile, highlighted the importance of protecting children's privacy in today's online world. The impact of our investigation into this widely used platform went far beyond a report. It also enabled the company to implement improvements to its privacy practices in the best interests of its users, especially children.

I recently announced an expanded investigation into the social media platform X and its Grok chatbot. This investigation will examine the emerging phenomenon of AI being used to create deepfakes, which can present significant risks to Canadians.

● (1540)

[*Translation*]

These are just a few of the many examples that show the importance of privacy for current and future generations. The examples also illustrate how prioritizing privacy is a strategic and competitive asset for organizations.

That's why it's so important to modernize the legislation so that we can have modern laws to help businesses make sure they have adequate protections.

[*English*]

For organizations, embedding data protection into programs and services can enable responsible innovation, facilitate global operations, improve data security and mitigate risks, including of major breaches. Modernizing privacy laws aligns with Canada's ambition to support growth, to seek opportunities with partners around the world and to continue to be a voice of modern progress, setting the stage for a safe and secure digital future for Canadians and Canadian industry.

[*Translation*]

Bill C-15 includes clauses that would amend the Personal Information Protection and Electronic Documents Act to include a right to data mobility to facilitate information sharing among all economic sectors. I support efforts to introduce the right to data mobility in Canada.

A right to data mobility would give Canadians greater control over their personal information and let them decide who their information can be shared with. It would also make it easier for them to switch service providers and choose the organizations they want to deal with. These are important considerations in building trust in today's digital economy.

[*English*]

Enhancing data mobility provisions can also support economic growth in Canada. For example, it would help promote competition and innovation by allowing individuals to take advantage of new business models, like consumer-driven banking, and by encouraging new players in the market, therefore helping to support small and medium-sized organizations. Specifically, Bill C-15 would add a new division 1.2 to PIPEDA that would require an organization, upon an individual's request, to "disclose the personal information that it has collected" from them to a designated organization. This right would be subject to regulations and would only apply "if both organizations are subject to a data mobility framework."

Bill C-15 would amend PIPEDA to provide the Governor in Council with the authority to make regulations regarding data mobility frameworks. These regulations would cover key aspects of a mobility framework, including safeguards and technical parameters for ensuring interoperability. They would also specify which organizations are subject to a framework and would provide for exceptions to the requirement to disclose information.

[*Translation*]

Given the scope of the issues that will be regulated, the office of the commissioner absolutely must be consulted by the government as the regulations are developed. I look forward to working with the government on these important issues.

With that, we look forward to your questions. Thank you.

The Chair: Thank you very much, Mr. Dufresne.

[*English*]

Okay, colleagues, we'll enter into our lines of questioning.

Mr. Guglielmin, the floor is yours for six minutes.

Michael Guglielmin (Vaughan—Woodbridge, CPC): Thank you, Chair.

Thank you for your testimony, Commissioner.

In division 23, under part 5 of Bill C-15, there is proposed section 10.4 of PIPEDA, which is on this proposed data mobility framework. This framework is intended to grow out of regulation. In other words, it will be bureaucrats, not parliamentarians, who have oversight over its development. Do you believe this introduces transparency concerns around the way in which Canadian data is handled?

Philippe Dufresne: I believe that my office should be consulted in the development of those regulations. That's why I'm setting out my expectation here, as I did in the other place when I appeared there to discuss this.

I think the legislation provides for the framework and the important topics, safeguards and parameters, and it specifies organizations and exceptions. For my role in this, I will be reaching out to the government to make sure that my office is consulted, and I expect this to not be an issue.

Michael Guglielmin: Do you think transparency might be enhanced by amending the legislation to allow for provisions of the data mobility framework to be statutorily established?

Philippe Dufresne: That's a decision for Parliament to make. Certainly, there is always a balance between having elements in legislation, with more debate and more parliamentary accountability.... Having some elements in regulation allows for faster development and more adaptation, so it's up to Parliament to strike the right balance.

In this instance, I do not have concerns with the way it is provided. However, this is based on my expectation that the government will consult with my office in the drafting.

● (1545)

Michael Guglielmin: Do you think the overall transparency and, potentially, the efficacy of the legislation could be strengthened by requiring that the regulations governing the data mobility framework be published before they come into force?

Philippe Dufresne: The more we publish before it comes into force and consult with industry and the regulator, the more awareness industry and Canadians will have so they can prepare for the implementation and provide their feedback.

Michael Guglielmin: What do you think are the chief challenges with developing this framework through regulation outside of the immediate focus of the Canadian public?

Philippe Dufresne: I think the challenge is making sure you have something that will work for Canadians, that will work for industry and that allows key elements. We see some of that in the bill in terms of consumer banking, consent, safeguarding, and making sure that if there is a privacy breach, it is reported quickly to the authorities, to the regulator. There's a big role for the Bank of Canada in the banking sector to approve entities and report breaches.

I think it's going to be important for the Bank of Canada, my office and other affected entities and regulators to work together, and I look forward to doing that.

Michael Guglielmin: I'm going to switch over to where in your testimony you were talking about deepfakes. The government has now introduced legislation, Bill C-16, that is intended to criminalize the creation and distribution of intimate deepfakes. At the same time, we have experts like Suzie Dunn, assistant professor of law at Dalhousie University, who have warned that the bill's definition of "deepfake" may be too narrow to capture much of the harmful content currently circulating online. That includes platforms like X.

As the committee prepares to undertake a study on artificial intelligence more broadly, what recommendations would you offer to us to ensure that legislation more effectively protects Canadians' privacy and potentially provides meaningful recourse for victims who have already experienced non-consensual AI intimate images?

Philippe Dufresne: My overall recommendation is to modernize PIPEDA, to modernize private sector privacy legislation. That is a mandate of this committee. That is an area where the Minister of AI has said publicly that the government will look to introduce, at some point, modernized legislation. There were attempts in the past.

My main message is that we need to modernize and we need to give my office enforcement authorities. This is a major gap in the enforcement regime. I can only issue recommendations. I cannot issue orders and I cannot issue fines. We are standing out among international partners in this respect. That is an easy fix that Parliament can do. There are other elements that need to be modernized as well, but that would give me the enhanced tools I need.

In the meantime, I have been using and will continue to use existing tools to deal with those issues. That's what I did in dealing with Pornhub and that's what I am doing in dealing with the investigation of X and deepfakes, but the fact remains that I cannot issue orders at the end of those investigations.

Michael Guglielmin: I understand that xAI has recently indicated that it will geoblock content where it violates laws of a particular jurisdiction. However, there are many who would argue that this response comes after significant harm has already occurred. Victims of intimate deepfakes continue to live with the consequences long after content is removed or restricted.

Simply from a privacy and victim protection perspective, what does that say about the adequacy of current regulatory approaches, which often rely on reactive enforcement rather than preventative safeguards?

Philippe Dufresne: Well, I won't say too much on X, because I launched my investigation last week. We're going to proceed swiftly on it, we're going to use the tools and we're going to draw our conclusions on it.

I think there's a challenge, if I look to our concluded investigation of Pornhub on the similar and related issue of online-based abuse and the sharing of intimate videos without the consent of individuals in the context of revenge porn and other types of situations. We investigated. We made a finding that this breached privacy law. We made strong recommendations that there needed to be a solution from now on, forward looking, but what do you do with what has already been posted? We also wanted that to be taken down. We wanted the takedown mechanisms to be faster and to be user-friendly. The company refused to do that.

Now we are in Federal Court trying to enforce this, but it is slow and expensive, and in the meantime those images continue to be available. That's where amending PIPEDA and giving my office order-making powers and the ability to issue or recommend fines would allow a much more immediate remedy, which could then be challenged in front of the court. That's the challenge.

You're often going to have responsive complaints or proactive complaints. In the context of Grok, I initiated it myself, but what's important is that once those are concluded, you get a real and meaningful remedy if there has been a violation.

● (1550)

Michael Guglielmin: Thank you.

The Chair: Thanks very much, Mr. Guglielmin.

Mr. Bains, the floor is yours for six minutes.

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

Thank you, Commissioner, for joining us today.

My first question for you is, how will the government ensure that regulatory requirements for data mobility do not disproportionately burden small and medium-sized enterprises?

Philippe Dufresne: I think that is an important part of any new law, rule or regulation the government adopts. It's important to hear from industry. It's important that the department hear from industry. It's important that industry itself is able to make its concerns and realities known, and a small or medium-sized enterprise in particular.

From my standpoint as a regulator, I also need and want to know what the challenges of industry are. What are the hurdles? For regulation to be effective, it has to be practical. It has to be doable by small and medium-sized enterprises, and of course, it has to protect Canadians. Building in privacy at the outset and making sure that we have good frameworks, good involvement of the regulator and good dialogue with industry allow industry to build this in from the beginning. It's more effective, it's less expensive and it leads to more trust from consumers.

This is going to be key, in my view, in data mobility and consumer banking. Canadians need to trust this, and they will trust it if they can see that privacy is built in from the start.

Parm Bains: I have a question with respect to monetary penalties. You appeared before the Senate committee on banking, commerce and productivity, where you stated that you do not currently have “the authority to impose financial consequences” for a breach of liability. In your view, is a monetary penalty one of the most effective ways to ensure compliance, or do you have other ways that you would go about that when dealing with breaches of sensitive information?

Philippe Dufresne: I believe we need to use all of the tools at our disposal. The financial penalties, the orders and the enforcement should always be a last resort. We should always try to prevent, resolve, educate and work together, so that's what we're doing at my office. I'm trying to resolve things quickly and informally, with letters of engagements, commitments and compliance agreements.

However, in situations where there is a disagreement or a major violation, you need the capability to enforce and also, I would argue, the possibility of fines to help decision-makers, CEOs, boards and investors invest the necessary sums to protect privacy. If there's the risk of financial consequences, it gives argument to the privacy champions in those organizations to build protections for Canadians, so it serves everyone in the end.

I want the ability to issue fines. I hope to rarely, if ever, have to issue them, but the existence of that possibility will make it easier for my office to convince organizations to prevent issues and take the necessary steps.

Parm Bains: Part of the committee's responsibility is to establish recommendations. Maybe you could provide a set of recommendations with respect to data mobility safeguards that need to be put in place. How can we put those in place? How can Canadians feel secure that their information and data aren't going to be exposed when they're shared?

Philippe Dufresne: In terms of recommendations, we've highlighted a number of priority recommendations for law reform, which I think are relevant in the context of what you do to protect the mobility of Canadians.

You need to make sure there is strong enforcement if there is non-compliance. You need to make sure there is a proper assessment, whether it's a privacy impact assessment or privacy by design, and make sure you bring this to the forefront. There are good elements of that in Bill C-15 in terms of consumer-based banking and making the consent express and user-friendly. These are things we always recommend and want to see.

Things like preventing the identifying of privacy breaches are major challenges to society all over the world, not just in Canada, and we're seeing them increase in number and magnitude. I talked about the 23andMe major breach I investigated with my counterparts from the U.K. There was very sensitive genetic information, and hundreds of thousands of individuals were impacted. We need to work on that.

This also costs money to organizations, so it's bad for everyone. The regulations need to provide for good safeguards and good reporting mechanisms in consumer-based banking. They're talking about immediately advising the entity responsible. We need to do all of those things, and there needs to be good and strong collaboration between regulators when there's potential overlap, as there would be here.

I look forward to working with the Bank of Canada as I am working already with the Competition Bureau and the CRTC. Digital issues and mobility issues don't stop at the border of one regulator or even one jurisdiction, so that collaboration is essential.

● (1555)

Parm Bains: Can you expand on some of the other departments we have to work with? You talked about the CRTC and others. Does the information sharing among the different departments need more improvement? Can you expand on how that's working?

The Chair: Answer quickly, Mr. Commissioner.

Philippe Dufresne: Sharing information among departments is an issue that would fall under the public sector privacy law, and that also needs to be amended. Departments need to be able to share information among each other. If it's personal information, there should be safeguards, but departments should talk to one another when they're dealing with breaches, because that helps with prevention and helps to remedy them.

[*Translation*]

The Chair: I forgot to mention something at the beginning.

[*English*]

If you're not in the midst of using your interpretation earpiece, put it on the sticker in front of you to protect the well-being of our interpreters.

[*Translation*]

I'm reminding you because I'm pretty sure we will continue in French.

Mr. Ste-Marie, you have the floor for six minutes.

Gabriel Ste-Marie (Joliette—Manawan, BQ): Thank you, Mr. hair.

Greetings to all my colleagues, including our new colleague.

I'd like to extend a special welcome to the witnesses, Mr. Dufresne and Mr. Chénier.

Thank you very much for your presentation, Mr. Dufresne. You've already given us a lot of information in your answers. In my questions, I'm going to cover a hodgepodge of topics.

I'll start with the open finance part of Bill C-15. If you've looked at it, what do you have to say about the responsibility of the various players in the event of a data breach?

Philippe Dufresne: There are some good things in the bill. It requires immediate notification, which is very positive. The act that governs my duties, the Privacy Act, mentions sending a notice as soon as possible. I already recommended that it be strengthened, for example by saying that it must be sent within a maximum of seven business days. Here, we're talking about immediate notification. That's positive, and it also raises a question.

For example, if the Bank of Canada or other entities were involved, I could also receive a notification, because those entities would also be subject to the privacy regime. Therefore, we need to be able to work together. One of the themes I've been focusing on for a long time is that regulators should be able to share information among themselves when it helps them fulfill their respective mandates. The same theme arises when departments are victims of privacy breaches. Often, there is a slowdown because of the time it takes for the various sections to talk to each other, and it's the same thing for private businesses.

This is very important, and I think the bill is going in the right direction in that regard.

Gabriel Ste-Marie: Okay. Thank you.

I'll move on to another topic. Once again, this concerns data portability, and hence the authorization to transfer personal data from one institution to another. Bill C-15 concerns businesses under federal jurisdiction, but some businesses may be under provincial jurisdiction.

From your perspective, has the government consulted with its provincial counterparts on this to ensure alignment? Are the provinces, including Quebec, ready for harmonization?

Philippe Dufresne: I have nothing to provide about discussions or consultations between governments and between departments, because I'm not one of them. I can only assume they have taken place. I would be very surprised if there were no consultations between federal departments and provincial departments on these issues. That is certainly the standard practice in my area, which is regulatory bodies. I have a very special relationship with the Commission d'accès à l'information du Québec. This is exactly what we're talking about, because these are issues that will affect both levels of government.

Quebec has regulations on data mobility and portability. We also made a comparison when evaluating the bill. Some provincially regulated entities might want to be subject to the regime. Correct me if I'm wrong, but I believe it is also possible to recognize entities under provincial jurisdiction within the meaning of the framework.

However, ensuring coordination and interoperability with the provinces, including Quebec, will also be important for consumers and organizations.

● (1600)

Gabriel Ste-Marie: Thank you very much. Let's move on to another topic.

In your presentation and in your exchanges with one of my colleagues, you said that, in the divisions we're looking at, many parts of the bill would be implemented through regulations to be defined later. For us, as legislators, that's a leap of faith in the government. We put our trust in the government because regulations aren't voted on in the House of Commons.

You said that you assumed the government would consult you in developing the regulations, but I'd like to check something with you. Has the government made that commitment publicly, or does Bill C-15 state that the government will consult you and that you will be there to develop the regulations?

Philippe Dufresne: It's not written in the bill, which doesn't provide for a duty to consult us. It has not been the standard in other countries with similar legislation to provide for consultation with the Privacy Commissioner for that purpose. Australia is doing it, and I think it's a good thing, but it's not necessarily always done.

For my part, as I've said publicly in my testimony to the Senate and in other contexts, particularly when I talk to government officials, I believe that everyone stands to gain from planning this consultation, because it prevents certain situations. Ultimately, I'm accountable to you, as parliamentarians. If you ask me if I was consulted and I say no, that will raise all kinds of questions. Therefore, I say to the government that this is to everyone's benefit, that we are willing to be consulted and that Parliament can require it if it wishes to do so.

I set my expectations and I will continue to do so. If it's not in the legislation and the government doesn't do it, I will voice my concerns through annual reports and so on. However, I'm optimistic about it.

Gabriel Ste-Marie: Despite the optimism you've shown every time you've raised this issue so far, the government has never committed to systematically including you in the development of regulations.

Philippe Dufresne: I haven't heard any opposition either. It may not have been stated that there would be a commitment to do it, but I haven't heard anyone object to it either.

Also, I must say that, in the context of the potential legislative reform of the Privacy Act, for example, we had some good discussions with senior officials at the Department of Industry. So I think those relationships are going to get better.

Gabriel Ste-Marie: Thank you very much.

Thank you, Mr. Chair.

The Chair: Thank you, Mr. Ste-Marie.

[*English*]

Ms. Borrelli, the floor is yours for five minutes.

Kathy Borrelli (Windsor—Tecumseh—Lakeshore, CPC): Thank you, Commissioner, for being here today. I appreciate you answering our questions.

The new data mobility framework is meant to make it easier for people to switch services and increase competition. There isn't an outline for how this will work, and details like which industries are included, what data can be transferred, how it will be protected and who is responsible if something goes wrong will be decided later by the government.

It will be important for your office to be consulted by the government in the development of those regulations. Do you have faith that you will actually be consulted?

Philippe Dufresne: As I indicated to your colleague Mr. Ste-Marie, I am optimistic. I'm publicly setting out my expectations. I've done this in the other place, and I'm doing it here.

There is precedent, I would say, from the standpoint that Parliament amended the legislation on financial crimes and FINTRAC to allow more personal-to-personal information to be shared by banks among each other to identify fraud and terrorism financing. This led to the creation of a code of practice regime that is reviewed and approved by my office.

There is a precedent for positive, constructive exchanges. I'm optimistic that is going to happen, but I will certainly monitor it. If it does not happen, you will hear from me on it because I think it would be a disservice to the institutions, to the industry and ultimately to Canadians.

● (1605)

Kathy Borrelli: Thank you, sir.

We are seeing more and more attacks. We're hearing about more and more hacking, and consumers are left on their own to fight for themselves, with maybe a “sorry”.

Loss of financial data has far more dramatic effects on people's lives, especially if it gets into the wrong hands of criminals. When the breaches happen, what are the penalties, or what should the penalties be for those who do the breaching?

Philippe Dufresne: When we look at breaches, we're always looking at what measures were put in place, what should have been put in place, what lessons were learned and if there was inappropriate care for the personal information of Canadians, given the sensitivity, the risk and the attractiveness. Right now, there are no penalties, and that's the concern. In Canadian privacy law, there are no penalties at all.

This becomes evident when we compare ourselves to other regulators, including within Canada—my counterparts in Quebec now have the ability to issue fines—and internationally as well. When I investigated 23andMe for a massive breach of genetic data, my U.K. counterpart issued a major fine on the organization, because this was a situation where they had significant shortcomings and it led to terrible harms for individuals.

You're absolutely right that we should not be treating this as a technical matter. This harms real people in a real, significant way, sometimes forever, and it's difficult to chase that information.

There needs to be strong enforcement and strong consequences in appropriate cases. At the same time, we also need to help and work with industry. It's challenging. There are bad actors, and they're using AI and fast-evolving technology.

It's something we all have to work together on, but the gap in enforcement makes us weaker in that respect, and I think this can and should be changed.

Kathy Borrelli: The system for sharing data outside of Canada, as you say, is not as rigorous as it should be. Do you believe we need stronger legislation in that regard?

Philippe Dufresne: Sharing data outside of Canada is an area of my recommended amendments to privacy legislation. Right now, we have a general sense that if you're sharing data outside, you have to make sure, by contracts or other means, that you have an equivalent level of protection, but this could be more robust.

There are other jurisdictions that will call for a review of the entire legal system and where it's going and say, “Is there rule of law there?” Government access to private data is always a concern, because you can't have a contract that's going to prevent another government from taking information, so we need to strengthen that.

Kathy Borrelli: I need time for another question.

These things happen really quickly. Data mobility produces real-time risk. Is a complaints-based model sufficient for this kind of program, or can we do better?

Philippe Dufresne: Well, it's not sufficient, and that's why we need multiple tools. My preference is to take proactive action: to educate, to have frameworks, to have good regulation that is going to help industry do what's necessary, to have quick reporting if there's a breach and to have early compliance letters. I dealt with a big breach of information at PowerSchool, and we got the organization to commit very quickly early on to fixing it without the need for a long investigation.

You're going to need investigation in some cases, but it's a spectrum of tools. I agree with you that we should not always be reactive. We have to try to anticipate things, prevent things, create a culture of privacy and work with the good actors, but for the bad actors, we need more enforcement.

The Chair: Thank you very much, Ms. Borrelli.

Mr. Bardeesy, the floor is yours for five minutes.

Karim Bardeesy (Taiaiako'n—Parkdale—High Park, Lib.): Thank you so much, Chair.

There are a lot of important roles for your office in this legislation and these amendments. Do you feel you have sufficient resources to be responsive to the possibility of more public requests for your office to get involved in these issues?

● (1610)

Philippe Dufresne: We're monitoring all the potential new roles. In this instance, in this legislation, I'm setting out the need to be consulted in the regulations and to work closely with the other entities. I would not anticipate that will require many more resources.

However, overall, we have resource concerns at the OPC. We are in a time of restraint, as you know, with departments reducing their resources. We are in a situation where privacy challenges are growing and where the impacts of technology and the impacts of breaches—all those things—are growing.

My concern would be more about making sure that, even in a period of budgetary reduction, we are mindful of the context of privacy, where breaches, as a new mandate...and we have that as an increase. We are seeing the technology evolve and the data uses increase, so there are opportunities for Canadians. We're going to continue to monitor the situation to make sure we can deliver.

Karim Bardeesy: You referred to the data uses increasing. Probably all of us in the House and at this committee are concerned about the growing prospects for data use and about getting ahead of Canadians' understanding of what their ability is, for instance, to even be protected by this legislation. They may not have an awareness of it, or they may not be familiar with which frameworks might actually protect them and which ones they could freely contract into.

Could you speak to your understanding of Canadians' literacy on data protection frameworks and what we might need to do to elevate that literacy?

Philippe Dufresne: We certainly need to elevate it. We're seeing in our surveys increasing concerns from Canadians. Nine in 10 Canadians are concerned about their data and privacy and have a sense that things are moving quickly. Parents are concerned that their kids will not know how to protect themselves and their personal information.

We need to do more. I'm working together closely with the community here in Canada and around the world. Recently, we issued with provincial and territorial colleagues a resolution on educational technologies, making sure of what our expectations are in the use of educational technologies, making sure this is top of mind and in the best interests of the child, and making sure that parents and kids have a good understanding.

A lot of kids do. We just created a youth council at my office. I meet with youth to understand their perspectives, but they do feel that they're being surveilled. They're very knowledgeable—sometimes more than we think—about the technology, but they feel a sense that they're being asked for information and that it's challenging for them.

We need more of that. It will require the whole community in Canada and the international community as well.

Karim Bardeesy: Having sovereign data or protecting Canadian personal data within Canada depends on companies and markets that are sufficiently competitive so that you have options available in Canada or so that institutions, especially public sector ones, that might have limited resources can freely contract with entities that are able to provide protection in Canada and at an affordable price. Do you have any perspectives on that particular question as it stands right now?

Philippe Dufresne: I think the question of data sovereignty is a very important one, as is the question of competition and access. I think this is an area that government and Parliament need to reflect on, in particular in the context of privacy legislation.

I've recommended that one area of strengthening be cross-border data transfer. It's one of those areas of tension where, on the one hand, you need to protect data sovereignty and make sure that things that shouldn't leave a jurisdiction don't leave a jurisdiction. On the other hand, strong economies and international trade will require data transfers between jurisdictions. A good framework is required around that. That's why one of my priorities is to focus on that and make sure we have free data flow with trust and Canadians have better awareness and more transparency on that.

In terms of the decision on TikTok, one of our specific recommendations was to make much more clear, to which the organization agreed, the fact that the data of Canadians could leave the jurisdiction. Where is it going and what are the implications? People need to know that.

Karim Bardeesy: Thank you.

The Chair: Thanks, Mr. Bardeesy.

[*Translation*]

Mr. Ste-Marie, you have the floor for two and a half minutes.

Gabriel Ste-Marie: Thank you, Mr. Chair.

Mr. Dufresne, I'd like to come back to open banking, which involves both federal banks and fintech under provincial jurisdiction. What actually happens when the province and the federal government haven't harmonized? My concern is two companies playing hot potato, not being subject to the same legislation, and then the consumer being on the losing end.

● (1615)

Philippe Dufresne: That's why it's important to have these exchanges between departments, between regulatory authorities and between industry players. Having had discussions with civil society and industry lawyers, I can tell you that this is part of the challenges they tell us about and the questions they ask us. They say that it's important not only in Canada, but internationally as well. There are multiple legislative regimes in this area around the world. So what do we do?

For our part, we work closely with them and try to find some commonality. In some cases, we even conduct joint investigations. We did one into TikTok with our provincial colleagues. It also helps businesses, because they only have to respond to us once.

However, if there isn't enough integration and interoperability, people in the industry might certainly say that they will think of this as one law taking precedence over another, which could raise all kinds of less relevant questions for consumers. As far as privacy is concerned, if two laws can apply, I always recommend that industry comply with the most demanding one. That way, it will make sure it complies with both. However, sometimes industry doesn't agree to taking that position.

Gabriel Ste-Marie: Thank you very much.

Mr. Chair, my time is almost up, so I will stop here, to follow your instructions.

The Chair: That's kind of you. I gave you 45 seconds extra last time, so thank you for giving that time back, Mr. Ste-Marie.

[*English*]

Mr. Falk, you have five minutes, sir.

Ted Falk: Thank you, Mr. Chair.

Thank you to our witnesses. You've provided some very valuable information.

I have a German shepherd dog that does investigations very quickly, issues his report swiftly and has the ability to escalate. You're telling me that you're missing the ability to escalate. You issue reports. What happens?

Philippe Dufresne: That's right. I issue a report and I make recommendations on whether there's been an infringement of legislation. We work with the respondents and say, “We want to bring you into compliance. Here is what we think you should do.” In many cases, I'm happy to say, the organizations will agree to our recommendations. They'll implement, and then we can say this was well founded and resolved, or conditionally resolved. That's the goal, unless it's not well founded. That even happened in the TikTok investigation, where they agreed to all our recommendations. That's a good-news story.

In some cases, there is no agreement, such as in the Pornhub investigation, where the organization refused—refused to require the express consent of all individuals whose intimate images are posted and refused to have a takedown mechanism that was at the level we felt would be user-friendly and quick enough. Then we have to take the matter to the Federal Court. It's different from an appeal in that we have to prove the case from the beginning, starting from scratch. Then the Federal Court will make its decision on whether there has been a breach or not. It can then be appealed all the way to the Supreme Court of Canada. That brings significant costs and delays to everyone—my office, the individuals affected and industry. It also delays the outcome.

In the case of Pornhub, it means there is no immediate enforceability of the order. If we had the ability to issue an order, the order would be made and then the information would be taken down. There could be an appeal afterwards, of course, and our decisions may be overturned, but in the meantime, Canadians would be protected. It would be the most protective approach. Right now we do not have that, and it's a gap.

Ted Falk: You would say it's a significant enough gap that it should be addressed.

Philippe Dufresne: Absolutely. It should be addressed. We are standing out in the international community by not having this.

I'm grateful for the many times that organizations are going to agree to the recommendations, and that's a testament to them. However, as a legal regime, having something not enforceable that is so important to privacy, to individuals and to businesses that are, I would argue, part of Canadian values and necessary to freedom and democracy is a concern, and it should be fixed quickly.

Ted Falk: Your mandate in this legislation is being expanded, but you're not getting the tools to really do the job.

Philippe Dufresne: Right now, there's no bill. It's expanded in this context from the standpoint that now there's going to be data mobility, but you are correct. I will have no greater enforcement power as a result of this than I did before.

● (1620)

Ted Falk: On your enforcement, does that mean you always have to press legal charges, or do you go through the authorities to do that? Do you go to a minister to report it and say charges need to be pressed? What is the process?

Philippe Dufresne: No, I'm fully independent from the ministers. As an agent of Parliament, I report to you, to the House and to the Senate. I do not need that, but I need to take action in court and file applications with the Federal Court, with all of the necessary legal expenses that adds. I am like a prosecutor at that stage.

Ted Falk: In the case of Pornhub, where you found significant breaches, law enforcement didn't pick up the torch and assign you a prosecutor who did the work for you.

Philippe Dufresne: No. We're doing that ourselves. I have lawyers representing me in court as we speak, and we're moving this forward. We continue to try to convince the organization to adopt our recommendations, but if this fails, the only avenue is to pursue the court matter to the end.

Ted Falk: Inside this legislation, there's also a provision that allows ministers to waive laws without proper disclosure. I'm sure you have concerns there.

The Chair: Answer in about 30 seconds, Commissioner, if you can.

Philippe Dufresne: This is meant to allow the testing of technology and innovation and allows a suspension of legislation. We see that certain regimes have sandboxes. This is also very much an area where I would like to see regulator involvement. In many regimes, we see the regulators—my equivalents—involved in that. They participate in those sandboxes and are there to say “we have concerns” or “we don't have concerns”. That's not present in this current form.

The Chair: Thank you, Mr. Falk.

Mr. Ma, the floor is yours for five minutes.

Michael Ma (Markham—Unionville, Lib.): Thank you, gentlemen, for being here.

My first question is, does this legislation mandate that data reside in Canada as a first measure? In the case of data mobility, will there be explicit consent by the consumer around exactly where the data will reside so they know exactly where the data is going?

Philippe Dufresne: There is no requirement that it reside in Canada. That is not required here. It could be added through regulations, and it's something that I believe Parliament should be reflecting on in the context of privacy legislation overall.

I don't think you can have an absolute requirement that nothing leaves Canada from a trade standpoint, as that would significantly limit innovation and trade, but there are certain areas—national security or otherwise—where there is a need for greater rigour. That issue is very important.

Express consent with respect to the open banking part of the legislation is there. That is necessary, and indeed, there's good language that makes it understandable for consumers.

On the more general provision, this would be in regulation. It's something that I look forward to seeing be developed. It has certainly been a key part of our recommendations and the advice we give on privacy. Canadians need to understand what's going to happen. They need to be able to agree. Otherwise, they're not going to buy in and the system is not going to succeed.

Michael Ma: On the topic of data mobility, are there regulations now or in the proposed legislation to have data be encrypted in residency, as well as in transit, so that the data is always protected?

Philippe Dufresne: I believe these aspects are going to be defined in the regulations in terms of the extent of the safeguarding and the types of requirements you want to see. This is an area where you want the right balance: not making it too onerous for organizations, but at the same time and depending on the sensitivity of information.... The more sensitive the information is, the stronger the safeguards should be, and this has been a theme in our work dealing with privacy breaches. The more the risk and the more the consequences, the more the safeguards. It's important to get that right.

In fact, to help SMEs in particular, we've developed an online tool whereby individuals can provide us with a description of what happened in a breach. It will give them a tentative sense of whether it is serious enough to warrant notification to the regulator. It will help them, because it's not always easy when you're in this situation. I think something similar could be done in the context of the regulation.

● (1625)

Michael Ma: We know that a lot of websites, when including corporate requirements, tend to ask a lot of questions beyond the business transactions they're involved with. Is there legislation to mandate that you can allow only the collection of data that is relevant to a transaction?

Philippe Dufresne: That's one of the principles of private sector privacy legislation in terms of appropriate purposes: not going for more than what you need.

There's a specific example of this in the open banking legislation: the prohibition of what's called “screen scraping”. It indicates that you cannot for the purposes of providing a consumer in Canada with a product or service, use an interface or application to gain direct access to their data using their authentication.

This is an example of where you have that information for the purpose of authentication, but you shouldn't use it for another purpose. That's a good practice overall. If you want to use it for something different that's beyond the reasonable expectations of individuals, you should seek separate consent or make it clear in your policies.

Michael Ma: I have experience with screen scraping, from over 20 years ago. The challenge there is that when open banking allows this type of activity, it exposes seniors to more risk. Right now, if they're exposed through one banking account, that's a limitation, but once you get into open banking, criminals can access more than just a single account.

What provision is being included to help protect people from further exploitation?

Philippe Dufresne: I would point to the provisions on express consent in open banking that talk about how it's important that this be done and that it be understandable. There, too, there will be some specific regulations, and I think this is a great example of something we need to get right.

In a lot of our work.... For example, we're going to be in the Supreme Court in March for a case against Facebook where a big disagreement we have is, how clear is the consent provision? How clear is the privacy policy? Often, they're very complex. They're very complex even for lawyers and experts, let alone individuals who are busy and who are not experts in the field.

We need to do better across the board on this, in my view, but particularly, as you point out, for seniors, and also for children. For TikTok, we recommended specifically that the policies for children be described in a different way. For some of our own statements we've done with the provinces on the privacy of young people, we've published them in a more user-friendly way. I think that's always a good exercise.

Michael Ma: To go back to the beginning, you talked about—

The Chair: Mr. Ma, I'm sorry to cut you off. We're a bit over time.

Michael Ma: Okay. I'm so excited.

Voices: Oh, oh!

The Chair: We appreciate the testimony.

Thank you, sir, for being here. Thank you to both of you.

Colleagues, we're going to move to our in camera round in a moment, although while we are in public I did want to share some very sad news that I just received. Our former colleague and member of Parliament Kirsty Duncan has passed away.

Many of you worked with Kirsty over the course of the past number of years. She was a former minister who was responsible for science and innovation and was a wonderful individual with a great spirit. While we were together here publicly, I wanted to share that. It's certainly sad for colleagues in the Liberal Party, but beyond that, it's sad for all parliamentarians when we lose someone with whom we served or who served the country.

I just want to take a moment to send condolences to Kirsty's family and thank them and to acknowledge our debt of gratitude for the time that loved ones spend away from their families to serve the country. Certainly, at a time of loss, it's important to recognize how precious that time is.

I wanted to share that before we break to go in camera. We will come back here in a few moments to pick up on the rest of our business.

[*Proceedings continue in camera*]