



HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

44th PARLIAMENT, 1st SESSION

Standing Committee on Industry and Technology

EVIDENCE

NUMBER 090

Thursday, October 19, 2023

Chair: Mr. Joël Lightbound



Standing Committee on Industry and Technology

Thursday, October 19, 2023

• (1535)

[*Translation*]

The Chair (Mr. Joël Lightbound (Louis-Hébert, Lib.)): I call this meeting to order.

Good afternoon, everyone.

Welcome to meeting number 90 of the House of Commons Standing Committee on Industry and Technology. Today's meeting is taking place in a hybrid format, pursuant to the Standing Orders.

Pursuant to the order of reference of Monday, April 24, 2023, the committee is resuming consideration of Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts.

I'd like to welcome our witnesses today, from the Office of the Privacy Commissioner of Canada. First, we are hearing from Philippe Dufresne, Privacy Commissioner of Canada.

Thank you for joining us again today.

Next, we have Lara Ives, executive director, Policy, Research and Parliamentary Affairs Directorate, as well as Michael Maguire, director, Personal Information Protection and Electronic Documents Act, Compliance Directorate.

I thank all three of you for coming back. I'm confident that everything will go well today—I'm looking at my colleagues—and that we'll have a chance to have a normal meeting and benefit from your insights on Bill C-27.

Without further ado, Mr. Dufresne, I'll give you the floor for five minutes.

Mr. Philippe Dufresne (Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada): Thank you, Mr. Chair.

Ladies and gentlemen members of the committee, I am pleased to be back to assist the committee in its study of Bill C-27, Digital Charter Implementation Act, 2022, which would enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act, and the Artificial Intelligence and Data Act.

When I previously appeared before the committee three weeks ago, I delivered opening remarks about the bill and presented my 15 key recommendations to improve and strengthen the bill. Today, I want to briefly highlight and respond to the letter the Minister of

Innovation, Science and Industry sent to the committee on October 3, 2023, and to answer any questions that you may still have.

[*English*]

I welcome the minister's stated position on the amendments being developed with respect to the proposed CPPA, in which he seems prepared to agree with four of my office's 15 key recommendations, namely by explicitly recognizing privacy as a fundamental right; by strengthening the protection of children's privacy; by providing more flexibility for my office to use compliance agreements, including through the use of financial penalties; and by allowing greater co-operation between regulators.

I also note and commend his statement of openness to further amendments following the study by this committee.

I would like to take this opportunity to highlight other ways in which the bill should be strengthened and improved in order to better protect the fundamental privacy rights of Canadians, which are addressed in our remaining recommendations to the committee.

I will briefly highlight five of our recommendations that stand out in particular in light of the minister's letter, and I would be happy to speak to all of our recommendations in the discussion that will follow.

First, privacy impact assessments, PIAs, should be legally required for high-risk activities, including AI and generative AI. This is critically important in the case of AI systems that could be making decisions that have major impacts on Canadians, including whether they get a job offer, qualify for a loan, pay a higher insurance premium or are suspected of suspicious or unlawful behaviour.

While AIDA would require those responsible for AI systems to assess and mitigate the risks of harm of high-impact AI systems, the definition of harm in the bill does not include privacy. This means that there would be proactive risk assessments for non-privacy harms but not for privacy harms. This is a significant gap, given that in a recent OECD report on generative AI, threats to privacy were among the top three generative AI risks recognized by G7 members.

In my view, responsible AI must start with strong privacy protections, and this includes privacy impact assessments.

● (1540)

[Translation]

Second, Bill C-27 does not allow for fines for violations of the appropriate purposes provisions, which require organizations to only collect, use and disclose personal information in a manner and for purposes that a reasonable person would consider appropriate in the circumstances. This approach would leave the federal private sector privacy law as a standout when compared with the European Union and the Quebec regime, which allow the imposition of fines for such important privacy violations.

If the goal is, as the minister has indicated, to have a privacy law that includes tangible and effective tools to encourage compliance and to respond to major violations of the law in appropriate circumstances—an objective I agree with—I think this shortcoming surely needs to be addressed for such a critical provision.

[English]

Third, there remains the proposed addition of a new tribunal, which would become a fourth layer of review in the complaints process. As indicated in our submission to the committee, this would make the process longer and more expensive than the common models used internationally and in the provinces.

This is why we've recommended two options to resolve this problem. The first would be to have decisions of the proposed tribunal reviewed directly by the Federal Court of Appeal, and the second would be to provide my office with the authority to issue fines and to have our decisions reviewable by the Federal Court without the need to create a new tribunal, which is the model that we most commonly see in other comparable jurisdictions.

Fourth, the bill as drafted continues to allow the government to make exceptions to the law by way of regulations, without the need to demonstrate that those exceptions are necessary. This needs to be corrected as it provides too much uncertainty for industry and for Canadians, and it could significantly reduce privacy protections without parliamentary oversight.

[Translation]

Fifth, and finally, the bill would limit the requirement for organizations to explain, upon request, the predictions, recommendations or decisions that are being made about Canadians using AI, to situations that have a significant impact on an individual. At this crucial time in the development of AI, and given the privacy risks that have been recognized by the G7 and around the world, I would recommend more transparency in this area rather than less.

With that, I would be happy to answer any questions that you may have.

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

Mr. Perkins, the floor is yours.

[English]

Mr. Rick Perkins (South Shore—St. Margarets, CPC): Thank you, Mr. Chair, and thank you, Commissioner.

The protection and safeguarding of an individual's personal information in the digital world, and the artificial intelligence world we're evolving into, in my view must be protected from the abuse of businesses and what they may intentionally or unintentionally do with that information.

After eight years, this new Liberal privacy bill, which is flawed, introduced 18 months ago, sat for a year in the House before it was brought for debate. You are Canada's Privacy Commissioner, the guardian of privacy for individuals in this country. Did the Liberal government consult and involve you in the development of this bill before it was introduced in June 2022?

Mr. Philippe Dufresne: On this question, Mr. Perkins, the bill was introduced before I was formally in place as Privacy Commissioner. The bill was actually introduced the day the House of Commons approved my proposed appointment as Privacy Commissioner. I was not consulted or involved, certainly, before that with respect to Bill C-27, because I wasn't the commissioner.

I have since been making recommendations—

Mr. Rick Perkins: Was your office consulted?

Mr. Philippe Dufresne: I know that there had been ongoing exchanges with my office and the department with respect to privacy matters. I don't know the extent of the details that would have been shared with my office prior to my arrival.

Mr. Rick Perkins: Perhaps you or your colleagues could tell me, if you did share your concerns or what the Office of the Privacy Commissioner of Canada desired, what should be in this legislation to update it.

What were the four or five key things that the office communicated, before this bill was introduced to the House, needed to be in this bill?

Mr. Philippe Dufresne: My office made a number of recommendations on the predecessor bill to Bill C-27. One of them included recognizing privacy as a fundamental human right. Some concerns were raised with some of the definitions of things like appropriate purposes or the ways information was conveyed. There was an extensive list of recommendations tabled by my predecessor. That is on the public record. A number of those were considered and led to Bill C-27.

There are outstanding ones. In my submissions, I have highlighted 15 key recommendations. In the annex, we made reference to previous recommendations that have been made.

● (1545)

Mr. Rick Perkins: It appears, based on the fact that there are 15 things, many of which you say were on the public record in the previous iteration of this bill, that they were ignored by the government in drafting this bill.

Does the Liberal government ignore the Privacy Commissioner often in its recommendations on how to improve privacy law?

Mr. Philippe Dufresne: I view my role and the role of my office as promoting and protecting the fundamental privacy rights of Canadians and being an adviser to you, as parliamentarians, in making the decisions. With this in mind, I've made 15 recommendations. I have communicated this. My office did that, before I was commissioner, with its views. Some were taken up by parliamentarians, by the government, and some were not.

In this instance, as I indicated in my opening remarks, I'm happy to see that, at least until now, four of my 15 seem to have been taken up. I look forward and hope to be able to convince all of you, including the government, to take up the remaining ones.

Mr. Rick Perkins: After the bill sat for a year, I presume there was some.... The minister said before the committee that he finally reached out and had some discussions with you, or the department did. Two weeks ago he came here and admitted that his bill is very flawed in key fundamental areas. He is proposing eight major amendments, which he has not shared with the committee so far after two demands by this committee to produce those documents.

Has he shared drafts of those amendments with you?

Mr. Philippe Dufresne: No, he has not. I have the same information you have, which is the letter that has been tabled at this committee.

Mr. Rick Perkins: As the guardian of privacy in Canada, the Liberal minister was truly committed to having a bill that protected Canadians' privacy from the abuse of businesses in the massive data world that we live in. He wanted truly important and accurate legal wording to do what both you and your predecessor said on issues like fundamental rights being protected in proposed section 5.

Do you not think a reasonable person who is truly committed to that would seek the advice of the independent experts about what is the best way to do that?

Mr. Philippe Dufresne: I think we do have significant advice that we can offer. The ideal way would be for my office to be consulted as early as possible, as often as possible, with proposed privacy changes. I understand there are some issues about cabinet confidentiality as to what can and cannot be shared, but on the topics that are being considered—the themes, the issues—I agree with you that if we're able to give input at the front end, there's a greater chance for these issues to be resolved.

Mr. Rick Perkins: Draft regulations and input can always be shared publicly before going to cabinet, to make sure it's what is needed to achieve what it is without having to go through the bureaucracy of cabinet.

As for the fundamental right issue on proposed section 5, I don't buy that the preamble has any value since it's not part of the published statutes of Canada. The purpose section sets out the importance of the bill and what its goal is.

If the bill says a fundamental right of the protection of privacy is of equal value to an organization's ability to use that, isn't that putting the cart before the horse? Shouldn't an individual's privacy be more important than a business's ability to use it?

Mr. Philippe Dufresne: It should be. This is why I've recommended this explicit recognition.

As you know, up until now it was described sometimes as a privacy interest or as a right—there was some more tepid language, I suppose—and my strong recommendation was that we need to make this explicit. We need to recognize it is quasi-constitutional, as courts have said and as the international community has said, so that in the purpose clause—and I recommended adding it in the preamble as well as in the purpose clause, but you're right; the purpose clause is the key—if you use the words “fundamental right”, you are sending a signal to courts, to decision-makers, to me, that even when you are balancing this with other elements, such as the needs of organizations—which have to be considered; we have to have innovation at the same time—if there is a clear conflict, one should prevail, and it is the fundamental right that should prevail. This is why it's so important this is enshrined in the law.

I was encouraged by the statement of the minister that this is now the intent. It's certainly something I've been advocating for since day one.

• (1550)

Mr. Rick Perkins: Thank you.

[*Translation*]

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

Mr. Sorbara, go ahead.

[*English*]

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

Welcome, Commissioner.

Commissioner, on October 3, two or three weeks ago I guess it was, you provided keynote remarks to the Big Data & Analytics Montréal Summit 2023. I've had a chance to go through your remarks. In one of the sections, entitled “Law reform and the regulation of AI in Canada”, you reference changes to the CPPA and also to the AIDA. You also comment about being “encouraged by the introduction” of the bill and—I'll use my own words—the tone and direction of the bill. One of the comments you make is about the protection of fundamental privacy rights.

In terms of reading your speech on Bill C-27, the direction of the bill, you are encouraged.

Mr. Philippe Dufresne: I've called it a step in the right direction, so I am encouraged. I see a possibility for further improvements, and those are the 15 recommendations that I am making, but I have said it is a step in the right direction.

Mr. Francesco Sorbara: These are new terms, new lexicons, that are being introduced into our vocabulary on generative AI, if you can use that term. If you had to contextualize the risk—and you use the word “risk” quite a bit—to privacy, where would you rate that?

Mr. Philippe Dufresne: Risks to privacy are significant in the context of generative AI. That's certainly my view. It's the view of the G7 ministers.

I pointed to a recent report of the OECD in September of this year, in which the OECD canvassed all of the G7 digital and tech ministers about the top risks of AI—not just the risks, but the top benefits as well, because there are benefits in terms of productivity and so on. The top three risks in this report included privacy. The first one was disinformation and misinformation. There were risks to copyright. The risks to privacy were third, and you had risks of exaggerated biases and discrimination. Those are the top risks. I would agree with that categorization.

Mr. Francesco Sorbara: Thank you for that colour, because this bill in this committee is going to be a very good learning experience for me.

Would you state that Canada, with this legislation, is a first mover?

Mr. Philippe Dufresne: With AIDA Canada has the opportunity to be the first. There is legislation in Europe that is moving forward, and that is something that we've pointed out in our submission on Bill C-27. This is a positive step, and Parliament needs to get it right. What I'm highlighting in the context of AI, in particular, is that the AIDA bill would bring in significant proactive risk mitigation measures to deal with harms and biases. This is good, and these are important measures, but they leave out the proactive steps for privacy, which is in the top three risks. This is why I'm insisting on having a privacy impact assessment as a mandatory obligation in the privacy bill, to close this gap.

Mr. Francesco Sorbara: If I understand this—and I apologize if I don't understand it; you'll have to forgive me for that—that is why it's important to list privacy as a fundamental right.

Mr. Philippe Dufresne: Listing privacy as a fundamental right is certainly part of it and certainly sends the interpretive message about how this is to be treated. Having a privacy impact assessment as an explicit legal requirement is helpful to organizations, because they know what they have to do. We can provide guidance through regulation or through my office, so that industry get this certainty and can thereby know why they're investing resources in doing this. It's to protect privacy, yes, but it's also because there is legislative backing.

Mr. Francesco Sorbara: Okay. When you mention industry, I take it one step back and I think of the individual having a right to their privacy to whatever degree, not just with industry. It's also the signal to industry about how they should treat the individual's privacy. I tie that back to the personal responsibility of the individual but also personal responsibility tied into industry.

In terms of your comments on trans-border data flows, we obviously work and are connected through an integrated world, as we see on a daily basis, sometimes for good and sometimes not for no good, unfortunately.

How does the trans-border data flow, in your view, and how should we be thinking about that?

• (1555)

Mr. Philippe Dufresne: This is an issue that the international community is grappling with. In Bill C-27 you have provisions about making sure that other countries are providing similar levels of protections through contracts. Other regimes have more detailed rules about this, for instance, looking at the GDPR, which has the adequacy regime.

There are a number of models for that, and what's important is making sure that the privacy of Canadians is protected with the data that leaves Canada.

Mr. Francesco Sorbara: As somewhat of an accountant—I'm more of a finance person—I know that in accounting there is rules-based and principles-based accounting. With this type of legislation, is it better to go rules-based or principles-based?

Mr. Philippe Dufresne: It's principles-based, because it needs to be technology neutral. It has to be legislation that will stand the test of time. It's 20 years old, and the Privacy Act in the public sector is even older, so we need this legislation to keep up with fast-moving technology. We're talking about principles, but we also need in legislation some specific obligations, so that organizations and Canadians know their rights.

For instance, we take the safety of travellers in airplanes very seriously. We have predeparture safety checks all the time to make sure that this is done, and done proactively, not after the fact. I see privacy impact assessments as being the same thing. By making sure that on the front end you're looking at privacy, you're treating it as a fundamental right, and you're mitigating those risks not only after the fact.

Mr. Francesco Sorbara: Thank you, sir.

[*Translation*]

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

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

Mr. Sébastien Lemire (Abitibi—Témiscamingue, BQ): Thank you, Mr. Chair.

Mr. Dufresne, thank you for being here and for your constructive recommendations.

When you last appeared before the committee, you had this to say:

...I recommend strengthening the preamble and purpose clause to explicitly recognize privacy as a fundamental right...so that these important principles inform the interpretation of all aspects of the legislation.

However, as my Conservative colleague noted, the preamble does not have force of law.

Can you explain the motivation behind this recommendation?

Mr. Philippe Dufresne: Our recommendation is actually twofold. We feel that adding a preamble is a step in the right direction. It refers to international instruments and all sorts of things. You can look to the preamble in case of ambiguity, even if it doesn't have the binding force of a provision of a statute. So we recommended amending the preamble, but we also recommend amending section 5, which deals with the purpose of the act.

In the Federal Court of Appeal's decision in the case involving Google, where the application of the Personal Information Protection and Electronic Documents Act was at issue, the court explicitly said that it was in the purpose statement of a statute that the intent of the legislator could best be seen. So, yes, it's important that section 5 be amended.

Mr. Sébastien Lemire: Do you feel that recognizing privacy as a fundamental right positions Canada as a leader in protecting human dignity around the world?

Of course, one of our goals is to achieve the highest standards internationally. Does this bring us closer to the European standards, for example?

Mr. Philippe Dufresne: Yes, that brings us more in line with Europe's standards. In fact, the European Union's General Data Protection Regulation, or GDPR, explicitly recognizes that, as does Quebec's regime. In all my international meetings, there was a consensus: privacy must be considered a fundamental right. Yes, it's important for Canada on the world stage, but most of all, it's important for all Canadians. Not only is privacy, in and of itself, essential and fundamental—it's a vehicle for freedom—but it's also the foundation for other rights. It underpins voting rights, human rights, equality rights and so on. That's why clear recognition of privacy as a fundamental right is essential.

Mr. Sébastien Lemire: The minister has acted on some of your recommendations to protect privacy, but you made a number of them—15, to be specific. Are there other recommendations you'd like to underscore today, to shine a spotlight on privacy concerns? I'm obviously talking about the recommendations the minister hasn't necessarily addressed thus far.

Mr. Philippe Dufresne: Yes, absolutely.

I have a list, in fact. The minister said he wanted to implement four of the recommendations, which leaves 11 of the 15 we put forward. Of those, I mentioned five, in particular.

The first recommendation is requiring PIAs for new technologies that can significantly impact Canadians, like generative AI. In my eyes, that is a major gap in the bill. PIAs are required for other types of harm and bias, but not for privacy harms. That seems contradictory, since it goes against an OECD finding: threats to privacy are the top third risk. Privacy absolutely has to be prioritized.

The second recommendation is requiring organizations to be more transparent about decisions that are made using AI. As it stands, the bill sets out the right to an explanation, which exists in other regimes. That right, however, is limited to decisions that significantly impact people. I recommend removing that proviso, so that people have the right to transparency and an explanation when-

ever a decision about them is made, no matter how great the impact.

People in the AI world are worried. We are hearing that more and more. They need reassurance. There are huge benefits to AI. Personally, I think more transparency will help people understand what AI is and what it isn't, show them that they are protected by a robust privacy regime.

The third recommendation revolves around administrative monetary penalties. They are used only as a last resort. I'm not saying this because I want to see them used—I hope that won't be necessary—but I would like those penalties to incentivize decision-makers to make good decisions. There is a gap, though. Currently, one of the biggest violations in the bill is not subject to an administrative monetary penalty. I'm talking about contravening the provisions on legitimate business purposes. I think this is a major consideration.

The fourth recommendation deals with the broad regulatory authority being given to the government, specifically the ability to make exceptions to the act without having to demonstrate that those exceptions are necessary. That is overly broad, in my eyes. A provision in the bill even allows the government to make regulations to completely exclude an activity from the application of the act. That goes too far and must be rectified.

The fifth and final recommendation proposes the creation of a tribunal as another layer of review. This would lead to a longer more expensive process and require the creation of a new structure. This diverges from the regimes in Quebec, Europe and other jurisdictions. Here's what I recommend: if a tribunal is set up, its decisions should be reviewed directly by the court of appeal. That would add a layer of review while removing another. The other option is to follow other models by giving my office the authority to issue fines and making those decisions reviewable by the usual court, as is the case in most regimes.

• (1600)

Mr. Sébastien Lemire: Quickly, can you tell me whether you would welcome non-monetary penalties?

I asked that question before, and the department officials seemed amenable to the idea.

Mr. Philippe Dufresne: Currently, the bill gives my office the authority to issue orders.

Most cases would probably involve the use of orders instead of administrative monetary penalties. The bill does a good job of prescribing the use of penalties. It lists the factors that must be taken into account, including the organization's approach and diligence, and whether it complied with a certification program. Whether the organization acted in good faith really matters, as do the efforts it made.

My office has the authority to issue orders, which is extremely important. I think the penalties are high enough, but with the use of orders, it's possible to put a halt to the activity and the collection of the information. Both of those are very important. Persuasion and negotiation are also tools, of course. That's why we recommended the use of compliance agreements, something the minister agreed to. That ability is also very important.

My preferred approach is to use dialogue and to encourage organizations to make the right decisions before they go astray.

Mr. Sébastien Lemire: Thank you very much.

The Chair: Thank you, Mr. Lemire.

We now go to Mr. Masse.

[English]

Mr. Brian Masse (Windsor West, NDP): Thank you, Mr. Chair.

Commissioner, thank you for being here.

I'm sorry if I ask a question a second time. We had technical problems on this end over here, so I missed some of the testimony and so forth.

I did ask this of officials. The Competition Tribunal recently issued a \$9-million penalty on the Competition Bureau for doing its job. That's for the Competition Bureau doing what it thought was the right thing and exercising due diligence in looking at the takeover of Shaw by Rogers. I've been assured that this can't happen in this situation if such a tribunal were to be created. Is that accurate? I wanted to know if you had that same opinion.

Mr. Philippe Dufresne: My understanding of the situation involving the Competition Bureau is that the tribunal made an order for legal costs and expenditures in the context of that litigation. That is an ability that courts have in litigation. That is an ability that I understand the tribunal would have. My colleagues can confirm, but there is a proposed provision that the tribunal be able to award costs. That would be the tribunal in this instance.

• (1605)

Mr. Brian Masse: This is my problem with the government on this. I'm not even sure if they're serious about this bill anymore. We have a hard time getting in amendments. There's the drama that went around that. Maybe we'll get the amendments from your department tomorrow, if there's compliance. That's a thing that I asked directly. Hopefully we can have our own researchers and analysts test that out.

It almost makes it a moot point in many respects for the Competition Bureau and an independent public entity to be able to challenge the conglomerates and powers that be to go forward. In fact, the \$9 million is a drop in the bucket, if that was for Rogers. It's a squeeze on the Competition Bureau and clearly sends a chill down the spine of basically anybody who's interested in consumer rights in Canada. You can basically be bullied into the corner by a legal process.

That's good to know. I had some reservations about the tribunal to begin with. If that's the case, then this is much more abhorrent.

With regard to your 15 recommendations, could we walk through the five that the minister has agreed to in terms of those recommen-

dations? I want to make it clear for those who are here. Can you identify which 15 in what you've submitted here today are the ones the minister has agreed to?

Mr. Philippe Dufresne: Certainly. On the previous question, it is section 20 of the tribunal act that would give the ability to award costs in accordance with the tribunal's rules.

In terms of the recommendations that the minister has signalled agreement with, the first is the recognition of privacy as a fundamental right. In the annex of his letter, as I understand it, he mirrors my recommendation in the sense of recognizing it in the preamble and recognizing it in the purpose provision. That's one.

Mr. Brian Masse: That's number one.

Mr. Philippe Dufresne: The second is recognizing strengthened protection for children's privacy. This is one where I had recommended amending the preamble. The minister agrees and goes further. He proposes to amend clause 12 on "appropriate purposes" to include children's privacy there. I am supportive of that additional recommendation.

Mr. Brian Masse: That's number two.

Mr. Philippe Dufresne: That's number two.

Number three is to provide more flexibility for my office—

Mr. Brian Masse: Without going into details, would it be one, two, three, four and five? Is that how you stacked your document to us?

Mr. Philippe Dufresne: I was listing them in the order that the minister had them. If you prefer, I can give you the numbers in my recommendations.

Mr. Brian Masse: Yes, I would like that.

Mr. Philippe Dufresne: My number one recommendation on fundamental rights has been accepted. The number two recommendation on children's privacy has been accepted.

Recommendation number 12 is to "provide greater flexibility in the use of voluntary compliance agreements to help resolve matters".

Recommendation 15 is not explicitly in the annex. I take it from the minister's testimony and from the overall mentions in his letter that he is open to coordination and co-operation between regulators. That is number 15.

I understand—

Mr. Brian Masse: That's a possible number four.

Mr. Philippe Dufresne: That's right.

Mr. Brian Masse: As my previous question about the tribunal blows that potential, we'd really have to figure that out, because I was told that it wasn't the case, and now it is.

Is number five in here, too? Does it match up with any of your recommendations?

Mr. Philippe Dufresne: I've identified four. Those are the four—number one, number two, number 12 and number 15.

The minister did allude to other themes in his letter. He talked about the exceptions, but he was not as definitive.

Mr. Brian Masse: We know only that there are going to be three amendments coming forward, so it'll be interesting, because that doesn't even match up right there.

I'm going to be running out of time soon, so I'm conscious of that. Is there any possibility that we can get from you a ranking of your other recommendations?

I'm going to go through this and do the due diligence, but I'm curious as to where, in the professional opinion of the Privacy Commissioner and your office, there's a high level or degree of exposure or complications that need to be fixed, and maybe which other ones are less costly to privacy. I'm looking for almost a ranking of some sort that we can weed our way through, especially with respect to those that are coming forward.

• (1610)

Mr. Philippe Dufresne: I've given that to you today in my opening statement. I've listed five outstanding ones that the minister has not yet agreed to.

Mr. Brian Masse: Okay.

Mr. Philippe Dufresne: Those would be the top priority, starting with the notion of a privacy impact assessment for generative AI. To me, that is a major shortcoming.

If you look at AIDA and if you look at the minister's proposed amendments to AIDA, you see a lot of discussion about risk mitigation, identifying risk and managing risk. This is absolutely essential and critical. However, we need to do this for privacy as well as for non-privacy harms. I'm very much insisting on this.

The other important recommendation, which I would say is the top priority, is making sure that fines are available for violation of the "appropriate purposes" provision. This is a violation of section 12. This is the key central provision. This is at the heart of the bill in a way, but there are no fines for that. That, in my view, should be corrected. It's easily corrected by adding that to the list of the breaches.

Other comparable legislation, like Quebec's, for instance, simply says, "a violation of the law". The whole law is there. It's all covered. This approach lists offences, and then in Bill C-11 there were more omissions. It's been corrected to some extent, but it needs to be corrected further.

I talked about algorithmic transparency. It is an important element, especially at this time in AI. Again, we can manage that by providing guidance to industry, so it's something that's workable, but I think Canadians need to understand what is going on with their data and how decisions are made about them. If we limit it to matters that have significant impact, we're creating debates and limiting the transparency that Canadians deserve.

That is—

Mr. Brian Masse: I think I'm out of time.

Just in summary, here's what we've done. We have a bill here in which private bad actors have the capability of suing your commis-

sion, just like the Competition Bureau, and we've limited our fines and penalties on bad actors.

That's a perfect scenario.

Thank you, Mr. Chair.

The Chair: Thank you, Mr. Masse.

Before going to Mr. Williams, if you will allow it, colleagues, I'll grant myself a minute for one quick question to Mr. Dufresne.

Some hon. members: Agreed.

The Chair: There is unanimous consent.

[*Translation*]

I have a question for you, Mr. Dufresne.

If you were playing devil's advocate, what would you say is the best argument for a tribunal?

Mr. Philippe Dufresne: One of the concerns that's been expressed publicly, as I understand it, is that too much responsibility or authority is going to a single body, in other words, my office. Since the bill provides the authority to issue orders and significant fines, more procedural fairness may be warranted.

To address that concern, the government could say, yes, more procedural fairness is needed. That's the model used in Quebec and other parts of the world. You can't have the same process in a regime that includes fines and orders. The way the system works now, an investigation takes place and it culminates in recommendations. The level of procedural fairness isn't the same as that provided for in the bill.

Furthermore, the bill gives my office a new tool, the ability to conduct an inquiry. This tool ensures that procedural fairness and gives the parties an opportunity to be heard. It's something that exists in Quebec, British Columbia, Europe, Great Britain and France. The idea is that the commissioner can conduct somewhat of a more informal investigation at first, but once an order or a fine is issued, it becomes more formal and it moves up to the next level. That's where the procedural fairness comes in.

To my mind, following that model and allowing decisions to be reviewed directly by the Federal Court of Appeal wouldn't be an issue. The Supreme Court has recognized that an administrative decision-maker can have multiple roles. Obviously, it has to be managed properly.

That's my answer. I think the issue is the concentration of responsibilities or authority in one place.

The Chair: Thank you.

We now go to Mr. Williams.

[*English*]

Mr. Ryan Williams (Bay of Quinte, CPC): Thank you, Mr. Chair, and thank you, Privacy Commissioner.

I know there have been a lot of comments today about what the minister said and what's forthcoming. I want to make this very clear to those listening at home: This bill is very important because, for the first time in 20-some years, we're dealing with having the largest amount of data that individuals, including our children, have ever had out in the open. We're dealing with data and, of course, in the second section, with AI. It's not up to the minister to approve certain amendments or decide what he wants to give us. It's up to this committee and then the House of Commons to determine how this bill, if adequate, will go forth to protect Canadians. I want to make that very clear.

We feel that, as the bill is presented right now, this government has not taken privacy seriously. It has not listed privacy as a fundamental right in the “purpose” statement of this bill, which other subregions of the country, like Quebec, already do.

I want to speak today on a certain portion of this bill that already gives more power to business than it does to individuals. It's a section that I think you identified, called “legitimate interest”.

Commissioner, I'd like you to define “legitimate interest” in your own words for the public and for people listening. I know you have a legal background. It's your fourth recommendation. I want you to explain how this drafted bill continues to allow the government to make exceptions to the law by way of regulations, without the need to demonstrate that those exceptions are necessary.

• (1615)

Mr. Philippe Dufresne: The bill provides for some exceptions to the ordinary obligation to have consent and knowledge. It provides exceptions in situations linked to and necessary for business operations. There is a carve-out for activities that should not be for the purpose of influencing individuals. The bill recognizes there may be some instances in which businesses would need the information and it's not practical to obtain consent or advise individuals of it. The condition for this is that a reasonable person would expect the collection or use for such an activity.

I have a concern where the bill provides a list of activities that could be considered business activities in the act. Some of them are.... The first one is “an activity that is necessary to provide a product or service that the individual has requested from the organization”. There is that element of necessity. The second example is “an activity that is necessary for the organization's information, system or network security”. Again, necessity is there. The third is “an activity that is necessary for the safety of a product” or for the organization. This element of necessity is crucial, because that's what justifies the fact that you're going to get consent.

However, the fourth—this is at paragraph 18(2)(d)—says, “any other prescribed activity.” It means that the government can add anything in there without a requirement of necessity.

My recommendation is that this be limited by saying, “any other prescribed necessary activity”, or by making it clear that the government is always limited by that necessity test.

Mr. Ryan Williams: How hard would it be for you and your office to disprove claims to the collection and use of Canadians' data without consent under the “legitimate interest” exemption for business, as it's currently written?

Mr. Philippe Dufresne: The concern I have with this provision is not in our ability to prove or disprove something, or to make a finding on something. It's because, if you add an activity in this list, I am bound by that list. The courts are bound by it. If you add an activity in there that isn't necessary, it becomes an unnecessary exception to the rule of consent. It's one I would have to apply, because I am certainly bound by the law. I will apply the law, as will the courts. It means that, because of this paragraph, there is that risk or possibility. I'm not suggesting it's the intention of the government to do so, but the law would allow the government to carve out something that is unnecessary.

I think that should be reduced and limited to make sure the exceptions we have to the fundamental right to privacy are necessary.

Mr. Ryan Williams: Commissioner, answer yes or no: Are you comfortable that Bill C-27—in not defining “legitimate interest” for businesses, as it currently stands—allows the government to make lists of activities and regulations that would balance businesses over the privacy of individuals?

Mr. Philippe Dufresne: What I'm saying is that this is a problematic granting of authority to the government to carve out parts of the act.

Mr. Ryan Williams: Are you comfortable with how it's written right now, yes or no?

Mr. Philippe Dufresne: This section...I'm not comfortable with it. I'm recommending that it be modified so that the authority would be more narrow. As indicated in my submission, there's another section elsewhere in the act, which is highlighted in my submission, where, again, a whole activity can be removed altogether from the bill. The bill wouldn't apply at all. This is something that should be corrected to limit its scope.

• (1620)

Mr. Ryan Williams: Thank you, sir.

[*Translation*]

The Chair: Thank you.

It is now over to Mr. Turnbull.

[*English*]

Mr. Ryan Turnbull (Whitby, Lib.): Thank you to Mr. Dufresne and his team for being here. I appreciate your testimony today. I always found you, earlier when I was on PROC and had the chance to work with you and your office, to be very helpful and very good at communicating. I thank you for that. I appreciate your expertise. You bring a lot to this conversation that's very important.

We want to strengthen this bill and to continue to see it get stronger throughout, hopefully, what will be a collaborative working relationship for all of us.

Certainly, one of the top concerns I have is the rights of children. I know that you've spoken to this and written about this. Many children today, as we know, are immersed in the digital world. I can speak from experience. My 11-year-old daughter hides devices and is on many apps and downloading things. There are pop-ups, and she sometimes purchases things. There's data being gathered about her preferences, and this really concerns me. I think it concerns a lot of Canadians with regard to children's data and protecting their right to privacy.

Are there currently laws in Canada that help protect children's privacy online? That's the first question, and I'll have another one about this in just a second.

Mr. Philippe Dufresne: On the current privacy legislation, we've provided guidance in terms of how to obtain meaningful consent. In that, we talk about some things that should be looked at in the context of children.

My federal, provincial and territorial colleagues and I have recently issued a statement, a resolution, on protecting young persons' privacy. It gives examples of things that should be done and should not be done with the data of children, nudges them not to make a bad decision, and recognizes that they are more vulnerable.

We can interpret the law, to some extent, to protect children, but we need to do more, and this bill has started to do so. There is now a recognition in the initial version of the bill, and I give credit to Minister Champagne on that. This was in the original Bill C-27 as tabled—the recognition that the information of minors would be deemed to be sensitive information. That has impacts in a number of areas, in terms of disposal rights, and so on.

We took that, and in our recommendations, we recommended going even further than that to highlight the best interest of the child in the preamble of the bill, so that if there is doubt, in terms of interpretation, you can look at that. The minister has signalled his agreement with that and has suggested going further to include the special situation of children in proposed section 12 on interpreting appropriate purposes. That is a further improvement that I would certainly support. We see comments like that in the European context with recital 38 to the GDPR, highlighting that children deserve special protection. UNICEF has said that.

We know that our kids are digital citizens. They're spending time online for all aspects of their lives, including school. We certainly saw it more during the pandemic. It's important that the legislation protects them appropriately and protects them as children. We need to protect the best interests of the child. We need children to be able to be children in that world, to be protected, and not to suffer consequences later on, when they're adults, for things they have done online. There are improvements there, and I certainly support them.

Mr. Ryan Turnbull: When you say go further, I'm kind of interested. It's always a balancing act. Later, maybe we'll have a question about supporting innovation and balancing privacy rights. As we know with any of these tough issues and with emerging technologies, it's a balancing act. I'm interested. In your view, should

there be an extra set of fines or penalties for violations of the sensitive information that's collected on children?

Mr. Philippe Dufresne: The sensitivity of information is an element that's going to be considered in the bill. It's going to be considered. I have to consider that in how I conduct myself. The sensitivity of information impacts the form of consent, impacts the retention periods and impacts the security safeguards. Certainly, it's something to be considered, and it should be relevant.

The proposal by the minister, which I support, to add the special situation of children to the appropriate purposes clause, proposed section 12, is important. I would add to that my recommendation today to make sure that if you breach the proposed section 12, and if you breach the appropriate purposes, including by treating children's information inappropriately, there would be fines available for that.

Beyond that, with respect to children, I'm not suggesting more than what has been suggested in the recent proposals by the minister.

• (1625)

Mr. Ryan Turnbull: Thank you. I appreciate that.

The other thing that often comes up for me is thinking about how companies often collect information. We've heard stories about Tim Hortons collecting the location information of users of its app. I think it's concerning for many Canadians—to be tracked and not know how that information is going to be used. How could Bill C-27 prevent that from happening in the future?

Mr. Philippe Dufresne: Bill C-27 needs to prevent that to the same extent that the current law prevents that. As you know, this was a matter that my office investigated. We made findings that Tim Hortons had breached privacy law by collecting more information than it needed and by not being transparent about what was being done with that information.

We see these situations, and we've made some recommendations and some findings. Bill C-27 will help more than the current law, because it will provide for more explicit obligations in terms of explaining consent—making consent something that is explained in a meaningful way for individuals to understand. There is also the possibility that my office can issue orders, and there is the possibility of fines.

I believe that, in the Tim Hortons situation, the organization followed the recommendations. In the Home Depot decision that I issued last year, finding a breach of privacy, the organization agreed with the recommendation. However, that's not always going to be the case, so there need to be these enforcement tools—hopefully not to use them but to reach those results faster and in a proactive way.

Mr. Ryan Turnbull: What would the consequences be—

The Chair: Mr. Turnbull, you're out of time.

[Translation]

Go ahead, Mr. Lemire.

Mr. Sébastien Lemire: Thank you, Mr. Chair.

Mr. Dufresne, can you speak to how the fast-moving nature of technology creates significant challenges for privacy and data security? Could you see a technology sandbox being introduced? What I mean is requiring companies to deploy a new program in an enclosed environment before it's made available to the public, to see whether privacy rules are up to snuff.

Is that a requirement the bill could include?

Mr. Philippe Dufresne: Yes, absolutely. The use of sandboxes is good practice. Our British counterparts are very far along on that front. In the case of AI technologies, the industry gets to test out the data and methods in a secure environment.

It's clear that our office would have to be resourced to set up a sandbox. The bill doesn't go as far as establishing a sandbox, but it does require my office to provide the industry with advice as needed. That will be especially important for small and medium-sized businesses. Again, though, it will require capacity. The bill also calls on the commissioner's office to approve codes of practice and certification programs.

Those are all proactive and preventative measures. My recommendations on PIAs and privacy management programs are also prevention-oriented. That's the approach. Organizations have to do these things in the beginning and invest the necessary resources.

The OECD surveyed business leaders and legal experts to find out what challenges they were facing, challenges related not so much to AI, but, rather, to international trade. They said it was sometimes hard to know where to allocate resources because certain investments didn't yield any legal benefit or it was unclear.

Even if well-intentioned business leaders want to set up a sandbox, convincing shareholders to fund it is a challenge. Imposing a legal requirement on companies is helpful, because it sends the message that not only is it the right thing to do, but it's also required of them under the law. The same applies to PIAs.

By the way, I'm quite fond of the certification program provisions in Bill C-27. Europe has that mechanism, and what it basically does is encourage companies to develop the programs and seek the commissioner's approval. Doing this and following the process will help them when complaints arise, because it shows that they acted in good faith and were proactive. It could even lessen fines.

All of those measures encourage companies to move in the right direction. Incentives are extremely important. To encourage innovation and ensure that Canada is well positioned, we have to act on two fronts: impose fines in problematic cases, and reward and recognize good behaviour. They go hand in hand.

My office's mission is to promote and protect privacy rights, and I really appreciate that. It's about more than telling people they did something wrong after the fact. It's also about working alongside them to make sure things are done right from the start.

• (1630)

Mr. Sébastien Lemire: Thank you very much, Mr. Dufresne.

The Chair: Thank you.

Mr. Masse, you may go ahead.

[English]

Mr. Brian Masse: Thank you, Mr. Chair.

I'm curious as to how you think the Canadian model that's being proposed here measures against the American model. We're so tied with trade, and many of the companies are subsidiaries—one side or the other. I'm just curious as to whether you've had discussions with the United States. I know they don't have a privacy commission, but they have some other elements.

Could we perhaps have your thoughts on that?

Mr. Philippe Dufresne: We have a lot of discussions, in particular with the FTC in the U.S., which has jurisdiction for antitrust law. It is the equivalent of our Competition Bureau. Also, through that, it deals with privacy.

There's no national privacy legislation in the U.S. at the moment. There are proposals before Congress on this, but it's not moving forward. California has its own model, and they have some innovative mechanisms there to protect privacy. Nationally, there is no equivalent in the U.S.

We are in close discussions with those colleagues about AI. In fact, when I was in Japan last June, we issued a statement on generative AI. This was from all of the G7 commissioners for privacy, and for the U.S., that was the FTC. In that, we noted a few things. We noted that there are laws that apply to AI for privacy, and they need to be applied and they need to be respected. It also highlighted that we need to have privacy impact assessments. We need to have a culture of privacy when we're dealing with generative AI, because in many cases it is built on personal information.

There are a lot of exchanges that are going on in that space. I think the consensus is making sure that our citizens are aware that, yes, AI is moving at a fast pace, but we have privacy laws to protect citizens.

Mr. Brian Masse: There's nothing moving in the United States Congress right now. They can't agree on a lunch, let alone a Speaker, so there's not going to be a lot of movement there.

I guess what I worry about, though, in terms of the larger, broader picture, is the corporate influence on the United States' legislatures with some of the lobbying that can take place. We have a containment factor to a certain degree here, aside from persons being able to get some supports later on, but it's nothing near what the United States has. We just want to keep that in mind as we go forward with the United States.

You mentioned Japan. Very quickly, before I lose my time here, what about Europe? What are your connections there, and what is happening?

Mr. Philippe Dufresne: Yes, we're working very closely with Europe, with the G7 and the community worldwide.

I was at a meeting of the Global Privacy Assembly just last week, talking about ethical uses of AI and highlighting the fact that we need proactive, strong privacy protections.

Going back to the collaboration with the G7 again, working very closely together, we issued a statement on AI. I was pleased to see the statement cited in the voluntary code issued by the Department of Industry to deal with AI, reminding organizations that we currently have laws that apply and that have to be respected.

However, in this new bill, that's why I am highlighting that we absolutely need to make sure that protective, proactive privacy assessments are there, and that they are a legal obligation. Right now, in the public sector, there's no obligation for privacy impact assessments. It's in a policy of Treasury Board. Often we'll see that if those impact assessments are done, they'll be done later. Therefore, it's important to have that legal obligation.

I can tell you that the international community is very much focused on AI, as are the G7 ministers. As you said, the debates are going on in the U.S., but certainly what is being highlighted and noted is that you cannot separate privacy from AI. To protect AI, to deal with AI, to have guardrails, you need strong privacy protections.

• (1635)

[Translation]

The Chair: Thank you.

Over to you, Mr. Généreux.

Mr. Bernard Généreux (Montmagny—L'Islet—Kamouraska—Rivière-du-Loup, CPC): Thank you, Mr. Chair.

Thank you to our witnesses, as well.

Mr. Dufresne, the Liberals' new privacy bill was introduced 18 months ago, but it sat on the shelf for a year before they brought it to the House for debate. If I understood correctly, you didn't have an opportunity to comment on the bill in your capacity as privacy commissioner, since you took office when the bill was introduced. Your office did, nevertheless, have a chance to provide feedback on the bill.

Today, you told us that you made 15 recommendations. The minister proposed eight amendments, which you are no more privy to than we are. Here we are, asking you questions about a version of the bill that is by no means the last.

As the committee's proceedings continue over the next few months, do you expect to be able to give us your view on future iterations of the bill containing the Liberals' amendments? Knowing your opinion of the bill would help us in our assessment, especially since this is clearly not the final version.

On top of that, what do you make of the fact that the minister acted on only half of your recommendations? He accepted only four or five of the 15 you made. Why do you think he didn't accept more of them?

Mr. Philippe Dufresne: I think you'd have to put your last question to the minister to find out why he accepted certain recommendations and not others. To be clear, he did say in his letter that he was open to looking at others, further to the committee's proceedings. Beyond that, I can't speculate.

As for providing additional opinions, I would be glad to help the committee however I can be of service, whether it's commenting on proposed amendments or meeting with the committee again, later in the study, to answer other questions. It would be my pleasure.

Mr. Bernard Généreux: It's been said over and over again: this is one of the most important bills that will ever be brought before the House of Commons. It deals with something that is vitally important, protecting the privacy of all Canadians.

We have met a number of times to discuss this issue. It's crazy that we don't have the text of the bill today and that you aren't able to comment on the proposed amendments. We received a letter, but it doesn't contain the actual provisions that will appear in the bill. As you well know, words are crucially important in this case, especially as they relate to your first recommendation to recognize the fundamental right to privacy. Initially, it was included in the preamble, but now it will appear in the bill.

Mr. Philippe Dufresne: Yes.

Mr. Bernard Généreux: Like us, you haven't seen the final text of the amendments the minister refers to in his letter, but it's paramount that you share your views with the committee throughout our study of the bill.

Do you plan to do that?

Mr. Philippe Dufresne: What I can tell you is that I saw the proposals in the letter, but at the end of the day, I certainly have to see the actual text of the amendments to know where things stand.

Nevertheless, I can give you my views on what isn't in the letter.

The minister mentioned four issues on which he was prepared to move forward. I talked about the privacy right, which, as it's been described thus far, certainly seems to be more in line with my recommendation. That's also true for the protection of children's privacy, but we'll have to see the actual amendment. I have less information about the voluntary agreements, so I can't really say everything is satisfactory, since I haven't seen all the details. Lastly, he addressed my recommendation on co-operation between regulators.

Earlier, we talked about the Federal Trade Commission, or FTC, in the U.S. Under the bill, my office can work with the FTC on joint investigations—as we've done in the past—but we can't do the same with the Competition Bureau of Canada. It seems counterintuitive to me that I can co-operate more with other countries than with my own. That's something that will have to be resolved given the growing overlap between privacy rights, human rights, competition rights and copyright. We see that in the AI world, but elsewhere as well. Working together can be advantageous for everyone, Canadians and industry.

I did put forward eight other recommendations that the minister did not say he agreed with. I want to list them right now, since there's nothing on the table about—

• (1640)

Mr. Bernard Généreux: Allow me to interrupt.

Among the eight recommendations that have clearly not been taken up by the minister so far, which are fundamental and should find their way into Bill C-27?

Mr. Philippe Dufresne: Of my 15 recommendations, it would certainly be the sixth, which deals with privacy impact assessments. This is fundamental, because without it, we won't be assessing the privacy risks posed by artificial intelligence, even though we know they're significant. So that's the first recommendation I'd stress.

Mr. Bernard Généreux: What risks are you talking about exactly? Are you talking about the risks associated with corporate data collection?

Mr. Philippe Dufresne: I'm talking about all the privacy risks associated with data collection, use, retention, safeguarding, purposes, disclosure for purposes a reasonable person would consider acceptable, etc.

This must be taken into account in the context of artificial intelligence and an obligation must be provided for. The obligation to have a privacy management program already exists, but it needs to be more targeted. I liken it to the tests that are carried out before an airplane flight. You have to check the risks to privacy and the methods for managing those risks. It's very important.

The lack of monetary fines in cases where personal data is used for unacceptable purposes is also a shortcoming of the bill. This needs to be added.

You already have my list of 15 recommendations. I am therefore sharing with you those that have not been adopted by the minister.

The Chair: Thank you, Mr. Généreux.

Mr. Gaheer, you have the floor.

[English]

Mr. Iqwinder Gaheer (Mississauga—Malton, Lib.): That's great. Thank you, Chair, and thank you, Commissioner.

Canada's privacy legislation is 20 years old. During that time, we had Facebook come about. We had the iPhone released. We had social media become prevalent. It's actually very alarming that we haven't updated it in 20 years.

I come from the generation that was very young when, for example, Facebook was released. I think individuals—I'm not in that category, by the way; I was very careful—posted information that they perhaps did not want to, especially looking at it in hindsight.

We know that in the new legislation, there's an expansion of the personal information that individuals can request be disposed of. What do current laws cover, and how does the bill strengthen the ability of Canadians to have their personal information disposed of?

Mr. Philippe Dufresne: On that point, one of the issues in the bill is that it allows a greater right to disposal of information, so that's a positive thing. In particular, vis-à-vis children, it creates a stronger right to disposal. There's the example you gave of posting something when you're a minor, and then, when you're an adult, wanting to take it down. There's stronger protection there.

One of the things I'm recommending, in fact, is making it even stronger, even for adults, because right now there's an exception in the bill that says the organization does not need to dispose of your information if it's keeping it in accordance with the retention policy and it's informed you of that retention policy. That doesn't apply to minors, but it applies to adults. We recommend that that be removed as an exception, because we feel it is a broad exception. If the organization tells you what its retention policy is, you don't have the right to the disposal of that information.

We haven't seen that type of condition in international models. I feel we should provide a greater right to disposal in this section.

Mr. Iqwinder Gaheer: How would the process work? I know what websites I use, for example, but perhaps I don't remember all of them. How would an individual who wants to dispose of some of that information even find out where their information is being stored? What if the company is defunct now?

Mr. Philippe Dufresne: There are obligations for organizations to proactively prepare privacy management programs and to share some information about them. If it's information online, the idea is that you would see it online, but there are obligations for organizations to make it as useful.... Obviously, if organizations see information about themselves and they have challenges finding where it is, they can reach out to my office and we can assist in seeing what's going on there.

That touches upon a point of transparency and making sure Canadians can understand what's going on, because not everyone is an expert in technology, yet we are living lives that are very much digital. Understanding what's going on, certainly with respect to AI, the notion of algorithmic decision-makers and....

We hear a lot of comments about that. We have our surveys of Canadians, and we see that Canadians are concerned about the protection of their privacy. I think part of the solution to that is communication, making sure that Canadians can understand what's going on, what the institutions are that protect them, what their rights are and what is being done with their information. Sometimes, we can have an impression that's worse than reality.

That's why I'm recommending that there be strong transparency. In the bill right now, organizations that make AI decisions about Canadians—if they have a significant impact—have to proactively explain the general processes of those decisions. They also have to answer questions if there's a request, but that's only if that decision has a significant impact on Canadians.

My recommendation is that if a Canadian asks for an explanation, they should receive the explanation, even if it doesn't have a significant impact on them. It still has an impact on them. They want to know what's going on. I think it's beneficial for Canadians to understand what's being done with their data.

• (1645)

Mr. Iqwinder Gaheer: That's great. Thank you.

My colleague, Mr. Turnbull, asked about the example of Tim Hortons, and how the app was tracking the data.

The example I want to reference happens all the time. I am in a room, and there might be a device in the room, and I am talking about a particular product with my friend. I'll go into the other room, where my computer is, and I'll go online and see an ad for that very product. It could be a very particular product at that time, so you wouldn't normally expect to see that ad appear.

What is this bill doing to protect Canadians from that? What penalties can companies face if they don't comply with these new laws?

Mr. Philippe Dufresne: That raises the whole issue of consenting to being tracked, and privacy by default. What are organizations doing, and what are they telling you those default provisions are? In my view, the default provisions should be privacy protective, certainly if you're dealing with minors. It's about making sure you have these protections in place, that you understand what they are, and that you can ask.... Again, it's that transparency. You gave a perfect example. You see this, and you want to know why you are receiving this. It's being able to get that explanation and to understand whether you have consented to this and how your consent is interpreted.

This is what we've seen in some of the investigations that my office has done, whether it's Tim Hortons, Home Depot or, more recently, Canada Post. It is the sense that Canadians don't know what's being done with their information, and sometimes there is a disconnect between what organizations believe Canadians agree to and understand, and what actually is going on.

That transparency that the explanation.... Again, it's the privacy impact assessments and consulting my office to make sure you develop these reflexes. Privacy is a priority. It's not something you do after the fact. You're designing and thinking. You need to think about innovation, absolutely, but they're not mutually exclusive.

When I was appointed, I said that privacy is a fundamental right, but it's also not an obstacle to innovation. It's not an obstacle to the public interest. We can have both. Canadians deserve to have both, and tools like this will help organizations get it right. My office will be there to help organizations get it right, particularly small and medium enterprises.

Mr. Iqwinder Gaheer: That's great. Thank you.

The Chair: Thank you, MP Gaheer.

MP Vis.

Mr. Brad Vis (Mission—Matsqui—Fraser Canyon, CPC): Thank you, Mr. Chair, and thank you to the witnesses.

The last time I spoke to you, I brought forward a motion to get some of the answers as to why the government presented a broken bill. I think we got some results, and we're seeing some productivity now: Some of that information has been provided, and I can see that it's been very useful to you as well, Mr. Dufresne, so that's positive.

Some of my colleagues already touched upon the changes the minister has mentioned regarding section 12 of the proposed act. I want to dig into that really quickly.

However, first off, as I understand it now, when the current form of the bill, which is broken, is amended, we're going to see a children's right to privacy defined in the bill. Is that correct?

Mr. Philippe Dufresne: Again, we'll wait and see what's being done, but what is proposed is to recognize in the preamble the importance of protecting children's privacy, so that will be there.

As well, the proposal is in section 12—

• (1650)

Mr. Brad Vis: We already know that it's going to be included in the preamble, but will a fundamental right to privacy based on the information we've been provided with be defined in the text of the proposed act?

Mr. Philippe Dufresne: What I understand the minister to propose, based on his letter, is to amend the preamble to recognize privacy as a fundamental right, and to amend section 5 of the proposed act to recognize that privacy is a fundamental right in the purpose provision of the act, which is stronger than the preamble—

Mr. Brad Vis: Good.

Mr. Philippe Dufresne: In terms of children, it's a similar approach, as I understand it, recognizing the importance of protecting the privacy of children in the preamble, but also in the proposed section 12, which is the "Appropriate Purposes" provision.

Mr. Brad Vis: Can we properly amend the proposed section 12 of the act without having a clear definition of what a "minor" is, and what constitutes a "child" in this legislation as well? Do we need those provisions to be amended before we can look properly at making changes to section 12?

Mr. Philippe Dufresne: The issue of the definition of a "minor"—and I know the question was asked in earlier meetings—is something that could be included in an amendment, perhaps with reference to the provisions—

Mr. Brad Vis: I'm sorry, I have only a little time.

Would it be your recommendation that we define "minor" in this legislation, to provide greater certainty for the protection of children when it comes to their privacy rights?

Mr. Philippe Dufresne: I would support that, to remove uncertainty. If you're not saying anything, the presumption to me would be that you use provincial ages of majority, but I don't see a harm in specifying it here.

Mr. Brad Vis: Thank you. That's very helpful.

The Library of Parliament provided us with a comparative document, and one of the areas they talked about was concepts of consent. In the context of children, can express consent really be provided when a child decides to download an app on their parent's iPhone?

Mr. Philippe Dufresne: Again, this is all part of the requirements in terms of the manner in which consent is provided and what will constitute valid, express consent. We've provided guidance on this. This is part of the guidance my office can provide, but, certainly, children's consent has to be looked at differently.

Mr. Brad Vis: Would you recommend that we define it clearly, so there's no confusion that the concept of consent is defined twice in this bill, once for adults and once for minors, if we decide to amend this bill to include a definition of minors?

Mr. Philippe Dufresne: I'd have to look at the specific wording of what's being proposed, but certainly—

Mr. Brad Vis: We might be relying on you to provide that wording, sir.

Mr. Philippe Dufresne: That's right. I'm happy to provide suggestions on that, if it assists the committee.

Right now, the way it is done is that it recognizes minors' information as sensitive, and then it uses sensitivity as a factor in a number of those things, including consent.

Mr. Brad Vis: I know, but again, the reason I believe these definitions are so important is that the definition of sensitivity can be muddled if we don't have clear definitions of what a child is in the first place according to this legislation.

I think the same concerns I have about concepts of consent could apply to concepts of erasure in the bill as well. If there is a concept of express consent for a child, how would that relate to erasure or the right to have data removed?

Mr. Philippe Dufresne: The concept in the data removal for children in this instance is that you may have consented to something as a child, as a minor—and there's provision for obtaining parental consent unless you're able to do it as a minor—but as an adult you may come to the conclusion that you no longer consent to this.

Mr. Brad Vis: Thank you.

On that first point, let's put this in context. Mr. Turnbull talked about his daughter and apps. I have children in a similar age category, and I have the same concerns. We've heard a lot of cases. In British Columbia, we heard about Amanda Todd, a young woman who took her life out of shame after she had exposed herself on the Internet. Imagine there's a young girl who exposes herself on some type of app or platform, and that app or platform does not provide the right to have that information removed quickly enough when she was a minor. Does this bill go far enough to ensure that minors' rights are protected in cases of severe sensitivity like the one I just outlined?

Mr. Philippe Dufresne: The bill provides for the minor, once an adult, to have that removed—

Mr. Brad Vis: But not as a child.

Mr. Philippe Dufresne: It's a minor as well. Minors' information doesn't fall under the exception that exists if there's a retention policy. There's greater protection to remove minors' information, and that's something the bill would do.

• (1655)

Mr. Brad Vis: Without a doubt, if that situation arose, do you believe this legislation is strong enough to address those very vulnerable situations?

Mr. Philippe Dufresne: I believe that the bill sets out strong disposal protections for the information of minors, and it will also be interpreted as such by my office, because sensitivity is a factor I have to consider.

Mr. Brad Vis: Do you believe, under this proposed legislation, that you have enough powers to go after that third party app that may be retaining sensitive information about a vulnerable child?

Mr. Philippe Dufresne: What I don't have right now is the ability to recommend—let alone issue—a fine in that situation, because the proposed section 12 is not part of the offences—

Mr. Brad Vis: Is it your recommendation to this committee that we give you the power, as the Privacy Commissioner, to issue fines quickly and resolutely in cases where children's rights and their vulnerability have been challenged or have been exposed, or...? You get what I mean.

Mr. Philippe Dufresne: My office has to be able to act quickly, so all the tools should be available.

Mr. Brad Vis: Right now, you can't act quickly if you wanted to.

Mr. Philippe Dufresne: We cannot in terms of fines. That's why we need the ability to have compliance agreements that would include financial considerations, to have purpose violations as eligible for fines and to adopt the tribunal situation so it doesn't add delay to the process....

Mr. Brad Vis: We don't want any delay, do we?

Mr. Philippe Dufresne: Delay is not desirable in the context—

Mr. Brad Vis: Is it your belief that a tribunal will delay your ability or the ability of people to have sensitive information wiped from the Internet?

Mr. Philippe Dufresne: My view is that adding a level of review to the process will add a delay and a cost, and so I've given two options to solve that.

Mr. Brad Vis: I see, so in certain cases, if we go with the tribunal route, that sensitive information for a child could be delayed in being removed from the Internet. It could be delayed if we go under the governance model currently suggested in the legislation.

Mr. Philippe Dufresne: I'm talking about this in the context of financial penalties. I will have under this bill the ability to issue orders, so there will be no delay to the order part. I can order an organization to stop a practice and to stop a collection, so—

Mr. Brad Vis: In other jurisdictions do privacy commissioners have the ability to lay criminal charges in cases in which vulnerable or sensitive information related to children is in question?

Mr. Philippe Dufresne: Criminal charges are not something that would be laid by a commissioner, here or elsewhere. That would be done by the police, but there are—

Mr. Brad Vis: Can a commissioner recommend to a relative police force to make those charges?

Mr. Philippe Dufresne: There are provisions whereby we can notify the authorities in that context, and one of my recommendations, in fact, is to amend the period of time for summary charges. Right now it's 12 months, and I'm recommending that that period be longer or that there be an extension possibility, because I don't want individuals to run out of time if the process takes longer.

Mr. Brad Vis: That's a good recommendation.

Thank you.

The Chair: Thank you, Mr. Vis.

Mr. Van Bynen is next.

Mr. Tony Van Bynen (Newmarket—Aurora, Lib.): Thank you, Mr. Chair. I'm finding these conversations very informative.

Commissioner, in your 2018-19 annual report, you made reference to having the authority to provide proactive inspection powers without grounds. My concern is that we don't need to worry about the good guys. It's the bad guys we need to be able to act quickly against.

What would be the advantages for the OPC of having proactive powers, rather than having to give an organization reasonable notice before performing an audit and when the CPPA is possibly already being contravened?

Mr. Philippe Dufresne: The recommendation on audits was one that was made for proactivity. It was this notion that with great

power comes great responsibility, so if you have authorities in cases where there may be an exception to consent for the use of information, there should be an ability to do what I think my predecessor referred to as “looking under the hood”, so having verifications. That's what the audit process allows.

There were concerns with the criteria for initiating an audit. I'm looking for the section in Bill C-27. My colleagues can point it out to me. At the time, under the existing legislation, it talked about having reasonable grounds to believe that the act had been violated, and there is recognition that that was too strict. The current proposal in Bill C-27 now talks about having been violated or being likely to be violated, as I recall, and I'll be able to correct that.... Proposed section 97 says:

The Commissioner may, on reasonable notice and at any reasonable time, audit the personal information management practices of an organization if the Commissioner has reasonable grounds to believe that the organization has contravened, is contravening or is likely to contravene Part 1.

So it has been improved in the proposal on Bill C-27. The test is not as reactive as it was before, because of this notion of “is likely to contravene”.

• (1700)

Mr. Tony Van Bynen: I think that speed to the audit is critical, particularly when we are living in a digital world and that can disappear very quickly.

That leads to my next question, on the fines that may be issued. What is the extent of the fines being proposed, and in your opinion, given the scope and the scale of platforms today, are the fines significant enough to have a meaningful impact. What additional authorities would you have? My concern is that the fine may simply be considered a cost of doing business, and they retain the data and continue the violations.

Could you clarify that, the scale of the fines?

Mr. Philippe Dufresne: I could, and as I think you heard, this was an issue that came up with the departmental officials. I would agree with the departmental officials' answer to that question, which was that they are comparable and in some instances higher than our comparators in Europe, in terms of the percentages. I'm looking for the sections. I think it's 4% of the turnover. If it's a fine, it goes up to \$10 million and 3% of the organization's gross global revenue, and if it's an offence, the percentages are higher.

That's comparable to what we see internationally, but there is also the possibility of issuing orders. I think the combination of those two tools is important and something to be monitored, but it's not standing out as being too small a percentage compared to international comparators.

Mr. Tony Van Bynen: Up until now, to what extent has obstruction been a problem for your department?

Mr. Philippe Dufresne: In terms of collaboration with my office, we treat individual complaints case by case. We've seen situations in which we're making recommendations and they are complied with. Sometimes they are not.

In terms of pure obstruction that would rise to the level of criminal offences, I'm not aware of any. It's something that, obviously, has to be dealt with in the legislation so that there is a tool or a mechanism if that occurs.

That ability goes to the necessity of having enforcement authority. If you have right now only the ability to make recommendations, that is useful if the organization agrees and complies. If it does not, then you don't have a remedy.

Mr. Tony Van Bynen: I'd like to go back to an earlier question. I'm not sure if I got a specific response on that.

Does the purpose of this privacy act place the rights of commercial interests on the same footing as personal interests?

Mr. Philippe Dufresne: Currently, if we look at proposed section 5, the purpose provision talks about the "rules to govern the protection of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use" and so on.

That's why I was concerned from day one about the need to recognize privacy as a fundamental right. It's to send the message that, yes, you have to consider those two things, but these are not equal things. Yes, you will do everything to have both innovation and privacy. In most cases, I am convinced that you can have those things. It's the same with public interest.

If there's a clear conflict that you can't resolve, the fundamental right should prevail.

Mr. Tony Van Bynen: Do you have an issue with the word "and" in the purpose?

Mr. Philippe Dufresne: I think that putting in the preamble a recognition of privacy as a fundamental right in this way, with this amendment, clarifies the superior nature of the right that we're talking about, which is consistent with the treatment of it internationally and by the courts in Canada.

Mr. Tony Van Bynen: How much time do I have, Mr. Chair?

The Chair: You have none, but I've been very generous with time for everyone, so if you want, you can...

Mr. Tony Van Bynen: I have just one more question.

We're talking about competition and the scope, scale and concentration of resources. The act doesn't distinguish between small and large companies in terms of obligations.

Is there a risk that this would be a competitive disadvantage in terms of the obligations that are being placed on small businesses?

• (1705)

Mr. Philippe Dufresne: It's crucial to ensure that the regime can be met by small and medium enterprises, absolutely. The bill provides for a role for my office in terms of guidance. It provides the ability to join in certification programs and codes of practice. It's something that has to be taken into consideration. It's certainly something that I'm very mindful of.

To the point on competition and privacy, this is an example in which you can have overlap between competition and privacy. We need to make sure that protecting privacy doesn't harm competition and vice versa. We've made recommendations to Parliament and to the department on competition law review, to make sure you are dealing with what we call "dark patterns", which are manipulative uses of language and psychological tools to incite individuals to make wrong choices, either from a privacy or competition standpoint.

This is why, in the last few months, my colleagues, the competition commissioner and the CRTC chair, and I created a digital regulators forum. We are working together to identify these areas of connection and interoperability. There are similar groups internationally. Our first focus right now, in our first year, is AI and making sure we are on top of those new developments.

This is why my 15th recommendation is to expand the scope of my office's ability to collaborate with regulators like these, in particular in the context of complaints. Right now I can't do that with my Canadian colleagues, but I can do it with my international colleagues.

Mr. Tony Van Bynen: Thank you. It's been very informative.

[Translation]

The Chair: Thank you.

Mr. Lemire, you have the floor.

Mr. Sébastien Lemire: Thank you, Mr. Chair.

Thank you, Mr. Dufresne. Your recommendations were already clear, but your testimony today makes them even clearer.

I'd like us to look to the future, since one of the obvious goals of the bill is to protect people over time.

With the emergence of quantum computing, what safeguard or oversight mechanism might be needed to ensure the effective protection of Canadians' information and data?

Mr. Philippe Dufresne: We need to make sure that the law will hold up despite the rapid evolution of technology, if not with it. There's a lot of talk about generative artificial intelligence right now. A year from now, it'll be even more powerful. Who knows? So the law has to be able to adapt. That's why the bill contains principles and doesn't talk specifically about generative artificial intelligence, for example, but rather about automated decisions. The definitions need to encompass all this and there needs to be flexibility for the government to set regulations and for my office to set guidelines so we can adapt to new technologies.

The recommendation we're making on privacy impact assessments is very important in this regard. Every time we develop something, we have to document it, assess the risks and carry out consultations, precisely to stay ahead of these technologies. This is one of my priorities, along with protecting children's privacy. We have to keep up with the evolution of technology. This measure makes it possible.

Another of our recommendations concerns de-identified information. De-identified information is defined a little too broadly, in my opinion, particularly in French. This definition must be very strict, because it limits legal obligations. In these definitions, we must also take into account the risk of "re-identification." The bill says that more can be done with de-identified information, and that if it's anonymized, the law doesn't apply at all. So there's a big responsibility that comes with that. These definitions need to be strict.

On the issue of de-identified information, I recommended that we take into account the risk of "re-identification," because technology evolves. If a piece of information is de-identified today, but in two or three years' time, thanks to technology, we'll be able to know again who it's linked to, we'll be right back where we started. This has to be able to evolve over time.

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

Mr. Sébastien Lemire: Thank you, Mr. Chair.

The Chair: Mr. Masse, you have the floor.

[English]

Mr. Brian Masse: Thank you, Mr. Chair.

Just going back with regard to the tribunal, you mentioned alternatives if we don't go to the tribunal. What would be the picture laid out from your design for that, if we dropped the tribunal altogether?

Mr. Philippe Dufresne: That would be the model, in fact, that exists in Quebec and that exists internationally. In fact, the GDPR—which, as you know, is the regulation that applies to the European Union—states that the DPAs, which would be the privacy commissioners, have the ability to issue fines. In the recital, in the description of this, they're talking about the DPAs issuing the fines, and they're generally reviewed by the courts. They list Estonia and Denmark as being exceptions, where they have to ask courts to issue fines because of the specifics of their legal structure.

The CAI, my counterpart in Quebec, has the ability to issue fines. They are reviewable by the normal court system. If there were no tribunal, this could work in the same way. Bill C-27, as drafted, already creates a more formal process for my decisions. It provides that the investigations happen at the front end. You try to resolve matters. If you don't resolve the matter, then it goes to what is called an inquiry, and I will have obligations under the law to adapt codes of practice and consultation with industry. Procedural fairness has to be an element of that, and at the end of the day, those decisions, if you choose as a Parliament to give the authority to my office to issue fines directly, would be reviewable by the Federal Court through the normal judicial review process. That's certainly an option.

On the other option, if the decision is to create a new tribunal, my recommendation is that if we're adding a layer of review, we

should remove one, so it should go straight to the Court of Appeal, otherwise there will be a cost.

• (1710)

Mr. Brian Masse: If we create the tribunal, that will create a conflict with the Quebec model. Is that not correct?

Mr. Philippe Dufresne: With which model? I'm sorry, but I didn't hear you.

Mr. Brian Masse: If we create the tribunal, that will create a conflict with the Quebec model. Is that not correct?

Mr. Philippe Dufresne: Well, it would be a different model. There would be a situation, and we would have to manage that in practice, because we do some joint investigations. As you know, we're currently doing an investigation on TikTok and ChatGPT. That's the case now, because right now I don't have the authority to issue fines or orders. They do, so that's something we'll need to manage.

Mr. Brian Masse: Thank you, Mr. Chair.

I suspect that's why we don't have the amendments in front of us.

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

I'll now turn to Mr. Perkins.

Mr. Rick Perkins: Thank you, Mr. Chair, and thank you, Commissioner.

We had a discussion earlier about the preamble having no legal binding, that it's a statement of intent and, once passed, doesn't appear in the statute in Canada. The purpose section, then, is very important. You just said in response to other questions that if you put "fundamental right" in and the word "and", "and" is there balancing against that, but that's okay. It still makes "fundamental right" prominent.

I'll go in a different direction on that. Let's assume that's correct. The Liberals are introducing into this bill a concept in privacy protection, the concept of a legitimate interest, the legitimate interest of the business—the big business and its legitimate interest to use one's data in a way in which it doesn't have permission to use it, and to allow it to use it even if it causes harm to the individual.

I would argue that proposed section 18, which introduces this concept, actually does not make the privacy of the individual of paramount importance. Proposed section 18 actually makes business interests more important, because a large business can ignore whether or not you gave it permission. It can ignore whether or not the information being used is going to harm you for its own legitimate interests, which are not always aligned with those of an individual.

Would you not agree that having that "and" gives that power in proposed section 18 much more weight, enabling them to ignore whether or not it's a fundamental right?

Mr. Philippe Dufresne: I've recommended a few things to address this in my 15 recommendations.

In terms of the preamble, we did—

Mr. Rick Perkins: I don't want to talk about that. I just want to talk about this issue. I don't have a lot of time.

Mr. Philippe Dufresne: All right. I think that goes to the recommendation on making sure that the business activities are defined very carefully, that they are all necessary, and that you remove the ability to make exceptions by regulations without showing that they're necessary. The recommendation, in terms of clarifying and highlighting the fundamental right, has to be in the purpose clause, but it should also be in a preamble in the law, not just in the bill but also in the law itself, so that when people read it, they have—

• (1715)

Mr. Rick Perkins: That takes away the power from Parliament and leaves the judgment in the hands of bureaucrats as to what the list is, because that's where regulations get made.

I would also argue that the Liberals are further watering down this issue. When you look at the terms of express consent in proposed section 15.... For those watching, express consent means I have to give you permission to use my data. The Liberals have designed a number of escape clauses from express consent that allow businesses to get around it. Those escape clauses in proposed section 18 allow them to get around it.

Also, in proposed subsection 12(4), in the purposes of the bill, it reads that where a business needs to use a person's information for a new use, it doesn't have to get the person's permission. It just has to record it somewhere. There's no need for consent from the person if the business uses it for a new use.

As we know, this is evolving rapidly. I got somebody's consent five years ago. I decide to use their stuff in a different way. I just have to record it somewhere now. I don't even have to tell the person I'm using it. It's a further watering down of the person's protection as a fundamental right, giving much more power.... When you combine it with proposed sections 18 and 15, the exceptions, and with proposed subsection 12(4), that's giving enormous power to a business to do whatever they want with that individual's data without their permission.

Mr. Philippe Dufresne: Proposed section 14 talks about new purposes and indicates that they must not use it for a purpose other than the one determined and recorded, unless the organization obtains the individual's—

Mr. Rick Perkins: Sorry, but that's not what proposed subsection 12(4) says. It reads:

If the organization determines that the personal information it has collected is to be used or disclosed for a new purpose, the organization must record that new purpose before using or disclosing that

It doesn't say that it has to actually get express consent. That's in the appropriate purposes and express consent sections. It doesn't say that you have to go back for a new purpose and get express consent.

Mr. Philippe Dufresne: On those purposes, one of the recommendations we've made is to make sure that the purposes are specific and explicit. It's important for Canadians to know why this is going to be used, and it's important that when you're collecting this information, Canadians have an understanding of what it's for and what it's not for, and that this is something they would be reasonably expecting. We need to make sure that it is used in those ways.

Mr. Rick Perkins: I have one last question, and this deals with individual privacy. There have been a lot of submissions already that ask about the ability to breach your privacy when you're put in a group. Group data management is a way, as a former marketer, that I dealt with data from customers. I put them into groups, customer segments; then I pitch to you, based on data, what's going on.

Should there not be some provisions in here that limit the use of group data for the protection of personal privacy?

Mr. Philippe Dufresne: You will no doubt hear views on that. We made recommendations on the predecessor bill in terms of inferences and treating inferences as personal information. I think that when you're talking about AI, we can see more and more ability to use information, maybe even de-identified information or anonymized information, then draw some conclusions about groups. I think that is certainly something to think about and consider. Those privacy impact assessments with AI, I think, become key to looking at that aspect. This is why our definitions on de-identification and anonymization are strict. Not everyone agrees with that. Some have said it may be too strict, but it takes it outside the law.

Mr. Rick Perkins: I've met with many professors and computer folks who have told me that there's no such thing as anonymized data. It's very easy to back out, so I have one last question.

This puts more important responsibilities on your office. The tribunal element probably puts more on as well.

Have you done estimates about what this is going to cost in funding for your department to do this level of...?

Mr. Philippe Dufresne: Yes, we have. The amount we came up with is almost a doubling of the current resources that we have. We would need an additional \$25 million per year to have the resources on the compliance side, certainly, but also on the proactive side. The discussion we've been having provides responsibilities to approve codes of practice and certification programs, and maybe there will be a decision to have sandboxes.

All this advice to organizations and SMEs will need to be resourced. The new process will need to be more formalized. The fact that there are more protections may well lead to more complaints and more judicial reviews and challenges, certainly at the front end.

• (1720)

Mr. Rick Perkins: Does that change if there isn't a tribunal as one of your options, or if you are given more authority to do compliance agreements with fines?

Mr. Philippe Dufresne: I think that the compliance agreements will help, because it will mean we can resolve matters. Again, it presumes that the organization will agree. A compliance agreement is a settlement agreement. If the organization agrees to pay the amount, then we can resolve it. If the organization does not, then there still needs to be a process that will go forward. I think the tribunal will have resources that have to be dedicated to that, if there's a tribunal to be created. If there isn't, part of that may have to be done by my office, but we'll certainly manage it as carefully as we can.

The Chair: Thank you very much. I'll now turn to Mr. Turnbull.

The floor is yours.

Mr. Ryan Turnbull: Thanks, Commissioner.

There's some really great conversation today. I really appreciate all the questions and the positive engagement here. I think this is really good for this work and this legislation.

I want to get back to a line of questioning that I started on and didn't quite finish.

I sort of take it that Bill C-27 and the minister's letter, which provides details, introduce new obligations for organizations and companies. It's also giving your office and you new powers, which I think are both positive.

One of the questions that keep coming up for me when considering what work you'll have ahead, once we hopefully get this bill through and strengthened in many ways, is whether there is enough around detecting non-compliance. It seems to me that it must be hard to detect who is not complying with these additional obligations that are being introduced in Bill C-27.

Can you speak to how you'll undertake that? I know you mentioned it with the last question about additional resources needed. I'm certain that's part of it, but could you speak to how you'll detect non-compliance when it does occur?

Mr. Philippe Dufresne: Yes, for sure.

Certainly, resources are part of it, because there are a number of things here, whether they are audits, certification programs, guidance or communication, to make sure Canadians can flag things for us. There's also the technological aspect. We have a technical lab at the OPC, where we are trying to stay ahead of the evolving technology, and getting those resources, that expertise and that understanding will be important. Using all those tools, compliance and the request for information, there are obligations in there where I can ask to see certain information of organizations or their privacy management programs.

Certainly we'll need something put in place so that we are not in a reactive mode but are aware of what's going on. I have to say, we have good engagements with representatives in industry and academia. I think this will continue, both in Canada and internationally, to make sure that we are hearing what the trends and concerns are and can act on them.

Mr. Ryan Turnbull: Just as a thought experiment—because I'm sort of testing this in my mind—I'm sure there are cases of bad actors who are not forthright in fulfilling their obligations in certain instances. I guess what I'm asking is whether you have sufficient

powers and tools to be able to really detect those nefarious activities where they may not, and intentionally may not, be living up to the obligations, even once Bill C-27 has passed?

Mr. Philippe Dufresne: We will continue to develop our technical abilities and our technical resources in terms of identifying things we see in the ecosystem. The bill will provide more powers to obtain information and to initiate audits. There is an ability for my office to launch investigations. We call them “commissioner-initiated investigations”. That exists. That's what we've done in the context of our TikTok investigation and in the context of ChatGPT.

We're going to continue to use all the tools we have. Legislation would place more obligations on organizations to proactively share their information. In terms of bad actors, we'll need to make sure we're proactively able to identify them, working with our colleagues.

• (1725)

Mr. Ryan Turnbull: Thank you.

Do you start an investigation only when you get a complaint, or how do you initiate or initially detect individuals—or companies, in most cases, I think—that are not living up to their obligations? Currently how do you do that? Also, in the future, how do you envision doing that? I assume that, with additional obligations and additional powers, there's going to be a lot more activity to monitor, and we want that. I think this bill enables that and is designed in such a way as to empower you to do that. However, I guess I'm just a little unclear as to what that process looks like.

Mr. Philippe Dufresne: We do not require a complaint from an individual to launch a matter. We have the ability to issue audits. We have the ability to issue a commissioner-initiated investigation. That can come from a variety of sources. It could come from the monitoring of media reports. It could come from monitoring industry experts and actors who could flag things.

We're going to continue to expand on these capabilities to do spot checks and to make sure about trends and concerns, but certainly this is something that needs to be proactive and not just reactive. We'll need to have the resources for it, because, as you say, the environment is vast, and there are a lot of resources outside of my office, including in organizations that we may need to be investigating. We need to have equivalent capabilities, then, to do our work.

Mr. Ryan Turnbull: I'm not trying to give you ammunition to ask for even more funds, but I suspect that there's a lot of online activity and a lot of data being collected, and I suspect that it would be very challenging to try to monitor and detect any breaches of the obligations that would be in Bill C-27. With respect, I think you have your work cut out for you in the future. I don't envy you that, but I appreciate the work that will be undertaken.

Maybe I'll leave it there for the moment on that.

I have another question or two. On the flip side of this—and I think my colleague Mr. Van Bynen asked some questions about this—what are the risks in going too far? By “going too far”, I mean are there risks within this legislation and this debate we're having, such that we could go a step or two too far and impede all of the positive benefits Canadians are getting out of the use of these online tools?

The data that's collected has enhanced our lives in a lot of different ways. There's a sense in which there's that balancing act between innovation and privacy, which you've already talked about. I guess I want to know specifically whether you see any risks in going too far. We really have been talking from the other side, about not going far enough on privacy rights. If we go too far, we might also stifle innovation. Would you agree with that, and are there any risks to that?

Mr. Philippe Dufresne: We have to strike the balance, but we have to remember that we are dealing with a fundamental right, so we need to start with that premise. We need to make sure we're protecting the fundamental right to privacy, because it's core to who we are as a society and as individuals.

Absolutely, though, we need to do it in a way that supports innovation. We need to do it in a way that puts Canada in a competitive situation and that allows Canada to work and trade on the world stage.

The good news, in terms of protecting privacy, is that it actually gives us economic advantages in many ways, certainly in terms of Europe and being recognized by that system as providing adequate levels of privacy protection. That's not just good for privacy; it's good for trade, because it allows our companies to trade with Europe in a better way.

There are benefits there, but absolutely we need to make sure, and you need to hear from industry. I've heard from industry. I have good dialogues with them. They may not always take the position I

do, and that's okay. However, I can tell you that we have regular discussions and exchanges. They will be coming in front of you, and they have a valid perspective to bring.

Mr. Ryan Turnbull: They do.

I was sort of leading up to this, which is interesting. With very much respect, I'll say.... As the Privacy Commissioner, advocating for the fundamental right of privacy, it seems to me that you might naturally be inclined to support one side of this debate. I can hear that you definitely appreciate the side of innovation and industry, which, in a way, is the minister's responsibility.

There also may be a flip side to this. Those industry stakeholders would express their position with regard to where we could go too far and limit the benefits that are also very important for this work. I wanted to put that out there.

Respectfully, I hope we can continue to have a very collaborative working relationship as we move forward. I would expect nothing less, because that's been the history so far in our working relationship.

Thank you very much for being here today. With great respect, I really appreciate your testimony.

● (1730)

[*Translation*]

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

Thank you, Mr. Dufresne, and your team for making yourself available again.

Voices: Hear, hear!

The Chair: It's not every day that our witnesses are applauded like that. It's a credit to you.

I thank the analysts, interpreters and support staff.

The meeting is adjourned.

Published under the authority of the Speaker of
the House of Commons

SPEAKER'S PERMISSION

The proceedings of the House of Commons and its committees are hereby made available to provide greater public access. The parliamentary privilege of the House of Commons to control the publication and broadcast of the proceedings of the House of Commons and its committees is nonetheless reserved. All copyrights therein are also reserved.

Reproduction of the proceedings of the House of Commons and its committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the Copyright Act. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the Copyright Act.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

Also available on the House of Commons website at the following address: <https://www.ourcommons.ca>

Publié en conformité de l'autorité
du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

Les délibérations de la Chambre des communes et de ses comités sont mises à la disposition du public pour mieux le renseigner. La Chambre conserve néanmoins son privilège parlementaire de contrôler la publication et la diffusion des délibérations et elle possède tous les droits d'auteur sur celles-ci.

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la Loi sur le droit d'auteur. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre des communes.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la Loi sur le droit d'auteur.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

Aussi disponible sur le site Web de la Chambre des communes à l'adresse suivante :
<https://www.noscommunes.ca>