HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

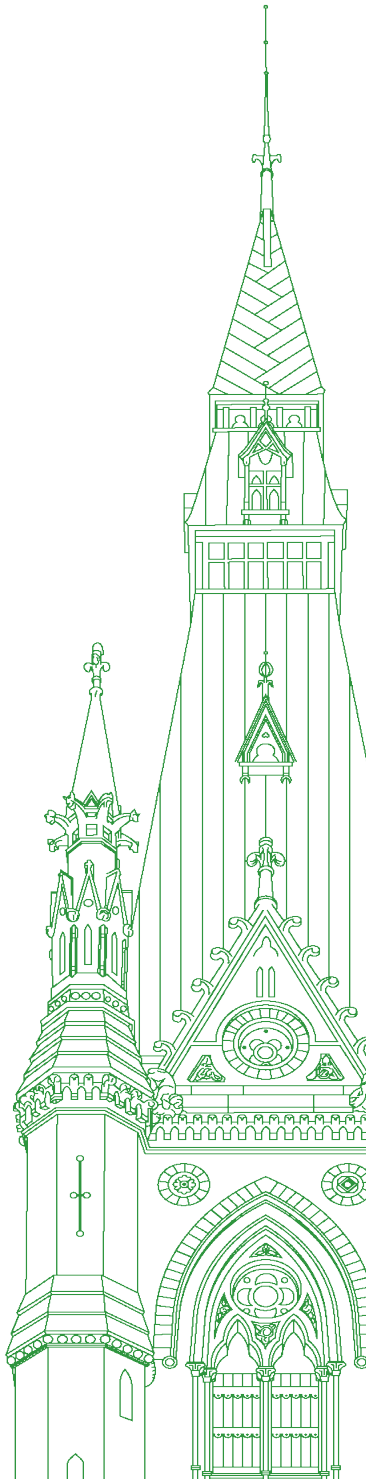
44th PARLIAMENT, 1st SESSION

Standing Committee on Industry and Technology

EVIDENCE

NUMBER 122

Monday, May 6, 2024



Chair: Mr. Joël Lightbound

Standing Committee on Industry and Technology

Monday, May 6, 2024

● (1105)

[*Translation*]

The Chair (Mr. Joël Lightbound (Louis-Hébert, Lib.)): Good morning, everyone.

I call this meeting to order.

Welcome to meeting number 122 of the House of Commons Standing Committee on Industry and Technology.

Today's meeting is taking place in a hybrid format, pursuant to the adopted order and the Standing Orders.

Before we begin, I would like to remind all members and other meeting participants in the room of the following important preventative measures.

To prevent disruptive and potentially harmful audio feedback incidents that could cause injuries, I remind all in-person participants to keep their earpieces away from the microphones at all times.

As indicated in the communiqué from the Speaker to all members on Monday, April 29, 2024, the following measures have been taken to help prevent audio feedback incidents.

All earpieces have been replaced by a model that greatly reduces the probability of audio feedback. The new earpieces are black, whereas the former earpieces were grey.

Please use only the approved black earpieces.

By default, all unused earpieces will be unplugged at the start of a meeting.

When you're not using your earpiece, please place it face down, in the middle of the round sticker on the table, as indicated.

Also, please consult the card on the table for guidelines to prevent audio feedback incidents.

Finally, the room layout has been adjusted, as you have been able to see since last week, to increase the distance between microphones and reduce the chance of feedback from an ambient earpiece.

These measures are in place to ensure that we can conduct our business without interruption and to protect the health and safety of all participants, including the interpreters, whom we thank.

I thank you all for your co-operation.

That said, we are holding a new meeting on Bill C-27.

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.

With that, I would like to welcome back the witnesses who are joining us.

Joining us today by video conference from the Department of Industry is Mark Schaan, senior assistant deputy minister, and here, in Ottawa, we have Samir Chhabra and Runa Angus.

Thank you for being with us today.

Before I begin, I would like to add the following.

[*English*]

Colleagues, just to remind everyone of where we were, we're still on CPC-7.

(On clause 2)

The Chair: There is a subamendment by the Bloc on the floor right now, which we were debating.

[*Translation*]

I will give the floor to Mr. Garon so that he can propose his subamendment.

Mr. Jean-Denis Garon (Mirabel, BQ): Thank you, Mr. Chair.

At the last meeting, we were at amendment CPC-7, and we had moved a subamendment.

Near the end of the meeting, after debating the subamendment for a few minutes, we understood that deciding what we would include in the definition of the term “sensitive” posed a number of difficulties.

So I sent everyone a proposal that should enable us to obtain the unanimous consent needed to amend my subamendment.

I could read it to you if you like.

● (1110)

The Chair: First, in order to withdraw Mr. Garon's subamendment that is currently being debated, the one that incorporated part of amendment NDP-6, we need the unanimous consent of the committee members.

Mr. Jean-Denis Garon: Allow me to ask a question. Is—

The Chair: You'll move your new subamendment afterwards. That will be simpler.

Mr. Jean-Denis Garon: Can I move it immediately afterwards?

The Chair: If you wish.

Mr. Jean-Denis Garon: If the committee members allow it, that would be a good way to do it.

The Chair: Do we have unanimous consent for Mr. Garon to withdraw his subamendment?

I see that everyone is in agreement.

(Subamendment withdrawn)

The Chair: Mr. Garon, I give you the floor to move a new subamendment to amend amendment CPC-7.

Mr. Jean-Denis Garon: Thank you, Mr. Chair.

I thank my colleagues for allowing this.

My subamendment would be as follows. Obviously, it is not in my party's nature to propose something in French only. However, to preserve the health of colleagues' ears, I will do so.

I move that motion CPC-7, proposing to amend clause 2 of Bill C-27 by adding after line 33 on page 5 a list of items, be amended as follows:

> Sensitive, in relation to information, includes any information about an individual, for which, the individual generally has a high expectation of privacy, which includes but is not limited to:
>
> a) Their racial or ethnic origin;
>
> b) Their political opinions, religious or philosophical beliefs, trade union or political membership, or political contribution history;
>
> c) Their sexual orientation or sexual habits;
>
> d) Genetic data or biometric data that can uniquely identify them;
>
> e) Their health condition, including any treatment or prescription on their medical record;
>
> f) Government identifiers, such as their social security, passport or driver's license numbers;
>
> g) Their passwords;
>
> h) Their financial data.

I guess it would be appropriate to provide some explanations.

First of all, we had discussed whether or not to introduce a list. I know that the government was a bit cold to the idea of introducing a list, but the amendment it had moved did in fact contain a number of items that were not presented as a list. In our subamendment, we're presenting them as a list.

Then we thought there were two points that needed to be clarified. First, there was the contextual nature—that is to say the consideration of personal information. I think Mr. Schaan talked to us about that. On the first line, we indicate that the individual must have a high expectation of privacy, which is not exactly the definition set out by the Supreme Court. This means that, sooner or later, it will be possible for an interpretation to be provided by the commissioner and by various courts.

We know that the European Union has set the gold standard for privacy. So we drew inspiration from the European Union's list, which included genetic and biometric data. This is of the utmost importance to us.

Of course, we consulted a number of stakeholders in various places. Like the minister, we don't say whom we consulted. I hope everyone will agree with that. It is impossible to alter biometric or genetic data once it has been stolen. If your biometric data has been stolen, that's for life. That is why, for us, it is of the utmost importance that this data be considered sensitive.

We also added union membership, which we felt went hand in hand with political membership, another element covered by the European Union.

At the last meeting, the officials discussed the issue of sexual orientation or sexual habits. We know that this information is a source of potential discrimination. We checked what the European Union has done, and it also considers this information to be sensitive. Obviously, I know that officials have different opinions, with all due respect, but it seems that things are working well in Europe. The economy has not stopped.

The last thing I wanted to talk about was financial data. In the European Union, financial data is considered to be subject to a high expectation of privacy. I checked that with some of my French friends. In the European Union, the banking system is still working, and people are protected.

There is obviously information that can go from one bank to another. This is information that, in many respects, is not nominative and that, when transferred, does not have a reasonable expectation of privacy. Examples include tax evasion or foreign accounts. These are all things that are subject to international conventions, to exchanges of information for which we don't have a reasonable expectation of privacy.

● (1115)

There will be a debate, and I think it will be very interesting. I had some difficulty with the argument that the banking system was going to stop working and that the banks would no longer exchange information.

We have before us the budget implementation bill, which will deal with open banking. For Quebec, it is obviously unacceptable for the federal government to impose rules on Caisses Desjardins.

The fact remains that, in this context, the exchange of information will be governed by the open banking protocol. In the context of privacy, we think it is appropriate to specify that financial information is sensitive. Of course, we are open to discussion, but please know that we have given it a lot of thought and believe that it is very likely that there will be a consensus on this proposal.

The Chair: Thank you, Mr. Garon.

The next speakers on the subamendment put forward by Mr. Garon are Mr. Masse and Mr. Albas.

Mr. Masse, you have the floor.

[*English*]

Mr. Brian Masse (Windsor West, NDP): As a clarification to make sure I have this right—and I may need some discussion with the researchers—is it “trade union” or just “union”? It might be a translation issue. It pops out because a trade union is often for the building trades or an additional layer of the skilled trades, which could be different from other unions. I'm just curious about that change.

On the lack of “personal information”, I'm not sure whether we need the word “personal” in there or not. That's one big difference.

I appreciate this constructive approach to trying to find a way forward, but those were the two things I'm curious about and would like to get specifics on.

[*Translation*]

The Chair: Thank you, Mr. Masse. That's a fair question.

[*English*]

On the question you're asking about trade unions, I note that in the original form of CPC-7, that was the language.

Is that a question for Mr. Schaan?

Mr. Brian Masse: Yes, but of course I'm always interested to hear Monsieur Garon's response too, in case he's done his research.

It's a question for both of them, quite frankly.

[*Translation*]

The Chair: Mr. Schaan or Mr. Garon, you have the floor.

Mr. Jean-Denis Garon: The intent was to include membership in a union or union activism. So we are going to use an expression such as “trade union” or “labour union”.

[*English*]

Mr. Brian Masse: Okay. That's what I thought.

[*Translation*]

Mr. Jean-Denis Garon: In case of doubt, the French version prevails.

[*English*]

The Chair: I don't know if it should be “labour union” or “trade union”.

I don't know, Mr. Schaan, if you have a word to say.

[*Translation*]

Mr. Mark Schaan (Senior Assistant Deputy Minister, Strategy and Innovation Policy Sector, Department of Industry): I would just like to add one thing, Mr. Chair. In Canada, the statute that regulates the establishment of a union is the Trade Unions Act.

[*English*]

In federal parlance, the current incorporating statute for unions is the Trade Unions Act. I wouldn't have specifics as to whether or not using “trade union” rules out other unions, but certainly the Trade Unions Act extends well beyond the building trades.

● (1120)

[*Translation*]

The Chair: Thank you very much for that clarification, Mr. Schaan.

I have on my list Mr. Albas, Mr. Turnbull, Mr. Vis and Mr. Williams.

Mr. Albas, go ahead.

[*English*]

Mr. Dan Albas (Central Okanagan—Similkameen—Nicola, CPC): Thank you, Chair.

I have just a quick question.

I sit on the Standing Joint Committee for the Scrutiny of Regulations, so I always keep a keen eye on French and English translations. I was hoping the officials could clarify the last part of the first sentence.

[*Translation*]

In French, it says “*qui comprend notamment et sans limite* ”.

[*English*]

In English, it's “which includes but is not limited to”. Is that essentially the same thing?

I have a follow-up question for Mr. Garon.

[*Translation*]

Mr. Mark Schaan: Mr. Chair, I will let my colleagues answer that question.

Ms. Runa Angus (Senior Director, Strategy and Innovation Policy Sector, Department of Industry): I think the word “*notamment*” is fine. Indeed, “ *notamment*” is translated as “included”.

[*English*]

Mr. Dan Albas: Thank you.

The officials are confirming that. I don't want to eventually see this at the scrutiny of regulations committee, where we'd have to quibble over whether it is the same.

In regard to this, I'd like to ask Mr. Garon something.

Referring to something that has not yet been identified is always a bit of a tricky thing. When you say there's an equal expectation of privacy and say “not limited to”, what kinds of things could this be referring to? We are counting on an interpretation by future bureaucrats and the minister responsible that allows them to determine what would have that status. I'm always a little loath, particularly after the Bill C-22 debacle, to give too much power of interpretation for future decisions without clarity as to what we're giving consent to.

[*Translation*]

Mr. Jean-Denis Garon: First, we include a list. Second, we're adding “but is not limited to”, for a very simple reason, which is that if this legislation had been in place 10 years ago, biometric data would not have been included. We would not have thought about it. Technology is changing rapidly.

The Supreme Court's interpretation of “reasonable expectation of privacy” is, as I understand it, subject to a legal test. We are introducing the notion of a “high expectation of privacy”. This concept could be interpreted later by the courts so as to expand the list as changes occur in the environment in which consumers and citizens operate.

In principle, this would enable the courts to interpret the notion of “high expectation of privacy” and expand the list as needed.

However, I don't think that it would change the minister's regulatory authority.

[*English*]

Mr. Dan Albas: I have respect for the work that's being done here. Obviously, I'm not a regular member. I'm not going to comment because this may have come up before.

This is why we usually have five- or 10-year reviews written into legislation. If other subjects are deemed important five or 10 years from now, I'd like them to originate from parliamentarians' review of things. That keeps the ball in Parliament's court rather than with someone who is making a recommendation and a minister who may have a much different value system from some of the parliamentarians elected to Parliament.

That being said, thank you, Mr. Chair.

I appreciate Mr. Garon's interventions today.

The Chair: Thank you, Mr. Albas.

Five- to 10-year reviews are a lofty ideal that isn't always respected. Mr. Masse could attest to that, but it's a nice ideal, indeed.

Mr. Turnbull, the floor is yours.

Mr. Ryan Turnbull (Whitby, Lib.): Thanks, Mr. Chair.

I want to thank Mr. Garon for putting something forward that attempts to combine numerous points that both parties had been making in the debate to find a path forward. I appreciate that. I also appreciate Mr. Masse's willingness to allow some of his thinking to be incorporated into an amendment, which is great.

[*Translation*]

Mr. Jean-Denis Garon: Mr. Chair, I would like to comment.

The Chair: Just a moment, Mr. Turnbull.

Mr. Garon, you have the floor.

Mr. Jean-Denis Garon: I just wanted to say that there is no French interpretation.

The Chair: Okay.

Apparently, there is no interpretation.

Mr. Jean-Denis Garon: Mr. Chair, the interpretation is working now.

[*English*]

The Chair: Mr. Turnbull, can you start from the top, please?

Mr. Ryan Turnbull: I was just expressing my appreciation for your work, Mr. Garon, and also for Mr. Masse allowing you to incorporate some of his thinking into the subamendment that you've proposed. This is great. It sounds like we're off to a constructive start.

I have a couple of questions.

One of the debates that we got into last time was around financial data. I know you've included it in your list. Intuitively, I think that financial data seems like it would be sensitive information. However, both the Privacy Commissioner and the Supreme Court disagree with that. They've said that the degree of sensitivity of specific financial information is a contextual determination. I could go on and quote them.

The Supreme Court decision of RBC v. Trang in 2016 has stated explicitly that in not all cases is financial information actually deemed sensitive, or the degree of sensitivity differs depending on the context of its use. Maybe I can go to Mr. Schaan to back me up on this, so that you're not just taking my word for it. The experts and officials are here with us for good reason.

Mr. Schaan, can you add anything to what I've said?

● (1125)

Mr. Mark Schaan: As it relates to financial data, I'll start, and then I'll turn to my colleagues to talk a bit about the treatment of financial data and information under the GDPR, because I know that was raised as a contrasting issue.

It's important to note that our system is somewhat unique in the sense that once a piece of personal information is deemed to be sensitive, it requires express consent, and it's not just express consent for it's collection; it's express consent for its collection, use and disclosure. That means express consent is required for its initial gathering from an individual and for its ongoing use. Then, when it needs to be disclosed to a party who is not the party who collected it, including in the process of business practices, express consent is required again.

Financial data and information is an extremely wide category. It includes transaction data. It includes information related to whether or not you hold more than one mortgage. It relates to a whole host of information that is, essentially, personal information that ties you to any type of financial transaction, of which there are many.

This would require express consent for every single collection, use and disclosure of that information. As an example, if I have an ongoing payment history with my bank and they need to use a third party processor, as many do for the purpose of continuing to use the transaction data, that would require express consent for every single one of the disclosures along the chain. It's not just when I first sign up for my bank account or even make the transaction; it is going to be required at every single step of the way. It is quite a broad category.

I think it's important to note the distinction between this express consent obligation and the varieties of ways in which processing and data information processing are allowed under the GDPR. For that, I'll turn to my colleagues, who can further enunciate why it hasn't gummed up the EU system. In part, it's because it's not understood in the same ways.

I'll turn it over to my colleagues.

Ms. Runa Angus: I'll take the question on the GDPR.

The GDPR refers not to sensitive information, but to special categories of personal data. Those special categories, in article 9 of the GDPR, refer to:

> ...racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation....

Those are the categories in the GDPR. As Mr. Schaan said, financial data is not on the list of sensitive information for the GDPR.

Mr. Ryan Turnbull: Thank you for that.

Help me understand this. We went through it last time, but what I'm asking myself is, so what? Why shouldn't we? Mr. Garon or somebody else might say that financial information is really important so we want it to be protected. The financial system wouldn't to come to its knees and be completely in ruin if we were to pass this particular subamendment, but I want to push back a bit on that and ask what the implications would be for the everyday, average citizen who is relying, potentially, on those third parties and on the financial information to be transferred in a way that doesn't present an imposition on the services they use and consume on a regular basis.

Mr. Schaan, I'll turn to you, and you can redirect to someone else on your team, if need be. Help us understand the impact of this. You've already said, to some degree, that express consent would be required at every single point along the chain of disclosure, but can you give us more detail on how this might impact everyday citizens?

● (1130)

Mr. Mark Schaan: To go back to first principles, it's important to note PIPEDA. One thing that will transfer over to the proposed consumer privacy protection act is an accountability principle such that collectors, users and disclosers of data will be accountable throughout the entirety of the life course of the personal information they've collected for its ongoing use and will be subject to the rules of PIPEDA as a function of those continued disclosures. It's one of the ways in which we ensure that in a data value chain, there is accountability throughout.

It's important to note that there is already quite a degree of responsibility placed on those who use, collect and disclose personal information. What "sensitive" will do, as I noted, is require express consent, notwithstanding the accountability principle. Across the value chain, there are a huge number of data transfers and disclosures that happen between entities that are not necessarily the same entity that did the first collection.

We've talked about banking, but even with retailers or others, there are often a significant number people. Your bank is using a third party like Interac, for instance, and then needs to transfer that information back to the host financial institution. If you used a credit card, for instance, a third party payment processor is often also involved before the information gets to your bank for the purposes of payment, and then it needs to be disclosed again to the original retailer for the purposes of clearing.

By buying an apple at the grocery store, you might see six or seven disclosures of personal information related to financial information, each of which would require the express consent of an individual for the payment and clearing of that one transaction. It becomes quite a lot when one imagines the broad category of financial data and the fact that we're now going to require express consent for every single step along the value chain, as opposed to relying on the accountability provisions of both the CPPA and PIPEDA and the rules associated with the use of personal information more generally.

Mr. Ryan Turnbull: We made the point in the last meeting we had that just because personal information doesn't all qualify as sensitive information doesn't mean that it isn't still protected and held to a very high standard. The CPPA is designed to do that. Obviously that part of the bill hasn't been contemplated by the committee yet, because it comes later. We're still on the definitions. We haven't gone into that, so it may not be as present in people's minds, but I think your point is well taken, Mr. Schaan, that the accountability principle is already baked into this bill.

Is financial information transfer already overseen by the Privacy Commissioner as well? Are there ways in which the Privacy Commissioner already has a role to play in overseeing that?

Mr. Mark Schaan: I'll turn to my colleagues, but I'll just say that all of the provisions of the act that relate to personal information and its usage are overseen by the Privacy Commissioner, subject to complaints and potentially subject to remedies.

I will turn to my colleagues just to be more specific about the powers that the Privacy Commissioner has over the use of personal information, not just sensitive information.

Ms. Runa Angus: As Mr. Schaan just said, the Privacy Commissioner has oversight over all collection, disclosure and use of personal information, which would include sensitive information. It would obviously include financial data as well.

The commissioner does a contextual analysis. Information that's not sensitive in one context may be sensitive in another context. Information together may become sensitive where individual categories are not sensitive. That's how the Privacy Commissioner looks at personal information. He determines whether it's sensitive or not and requires obligations that are commensurate with the sensitivity of the information.

The office absolutely looks at financial information. There are many cases where they have said that financial information is sensitive, and there are cases where they've said in another context that it's not sensitive.

● (1135)

Mr. Ryan Turnbull: Including all financial data as sensitive information—which is what this subamendment would do in the bill—would remove the Privacy Commissioner's discretion and his ability to issue guidance and use context as a way of determining the sensitivity of that financial data.

Is that correct?

Ms. Runa Angus: That's correct.

Mr. Ryan Turnbull: I see the answer is yes, but the microphone wasn't turned on.

To go back quickly, the GDPR categories that Ms. Angus read out did not include some of the things that are included in the list that Mr. Garon has presented in his subamendment. If I'm not mistaken, they only included up to paragraph (e), so paragraphs (a), (b), (c), (d) and (e). If we're really trying for interoperability and using the EU's GDPR as our standard—and that's part of the argument—then essentially we would be eliminating paragraphs (f), (g) and (h). When I read them, those were the things that seemed to carry some pretty high, potentially unintended, consequences.

Could we verify that the GDPR includes paragraphs (a), (b), (c), (d) and (e), but not (f), (g) and (h)? If I'm wrong, please feel free to correct me.

Mr. Mark Schaan: I'm happy to start and then turn to my colleagues.

Essentially, you're right. There are some considerations that should be brought to bear on some of the pieces of paragraphs (f), (g) and (h).

As we spoke about at the last meeting, it's specifically been noted by the Privacy Commissioner that in two provinces, driver's licence information is not actually deemed to be personal information. It's important to segregate the driver's licence—because that's not what this amendment says—from the driver's licence number, which is what is specified. There's lots of personal information on our driver's licence, for sure, but what's being requested to be considered sensitive is the driver's licence number, which in two provinces has already been deemed by the Privacy Commissioner to not be personal information. Therefore, giving it the status of sensitive information not only heightens that, but actually requires express consent.

We've already been over financial data, but passwords often also have context that potentially should be considered.

With that, I will turn to my colleagues to further elucidate some of the issues in the back end of the list.

Mr. Samir Chhabra (Director General, Strategy and Innovation Policy Sector, Department of Industry): As Mr. Schaan pointed out, the context dependency for any analysis of sensitivity of any information is critical. It's a cornerstone of the OPC's submission to this committee that we start with a context analysis of collection, use or disclosure of any information. That's really important because, while there may be some scenarios where it is somewhat rare for a category to be considered sensitive or not sensitive, the contextual piece is what gives the commissioner the ability to ensure that privacy is being protected at the highest level.

With regard to the EU's GDPR, as Mr. Schaan already pointed out, financial data is not included in Quebec's Law 25, nor is it included in the EU or U.K. GDPR. Similarly, the aspect of passwords is not included in any other jurisdictions—save for California, where it's referenced in a very specific manner, which is that your login information for a sensitive use case would be considered sensitive information because it's what the password and the user credentials give access to. That's the nature of the sensitivity there.

Including passwords overall, of course, as we explained the last time we spoke at committee, is simply because it introduces a degree of non-neutrality in dealing with technologies that could also be problematic in some cases.

As Mr. Schaan already pointed out, a driver's licence has been specifically ruled not to be personal information by the OPC in two provinces, so adding the designation of sensitive personal information to something that the OPC himself has said is not personal information at all would be somewhat of a conflict.

● (1140)

Ms. Runa Angus: I'll perhaps add a technical point.

The amendment also refers to social security information as being sensitive. Social security is not recognized in the Canadian system. It might be social insurance numbers, for example, that have been recognized by the OPC on many occasions as sensitive, but social security is not really a concept that exists in Canadian law.

Mr. Ryan Turnbull: Similarly, regarding the passport number, I assume by the way it's structured here, with the language of "government identifiers, such as their social security, passport or driver's license numbers", that it's really only referring to the numbers.

Is a passport number also sensitive? It's the same argument for a driver's licence. I assume passports have lots of personal information in them that should have a high bar, but is the number of the passport sensitive information? It seems that's the intention here.

Does the same argument that you made, Mr. Schaan, for driver's licence numbers also apply to passport numbers?

Mr. Mark Schaan: As Mr. Chhabra noted in the California instance, some of this is about what they're being used for and what they reveal.

In the case of Ontario, those of us who are citizens of this province know that our birthdate is included as the last six digits of our driver's licence number. That's not the case in a number of other provinces, so again, this is where context will matter.

In many of those instances, because of what you can potentially use a passport number for and the link back to the individual, it would probably be deemed personal information worth protecting. However, in and of itself, it doesn't necessarily suggest that the combination of numbers and letters is sensitive information, because, again, that's what it's for.

I think giving broad ambit to the commissioner to lay out and provide guidance around what can and cannot be done with this type of information and what protections need to be put around it—including, for instance, suggesting that express consent is the best approach in some of these contexts—is more important than just a broad categorization. Again, within that categorization are uses, contexts or, in fact, instances where it's not even necessarily personal information in and of itself.

Mr. Ryan Turnbull: Really, by including these in here, we're saying that context doesn't matter. In terms of determining sensitivity, we're saying to forget context; it's always sensitive information.

That's really the heart of the problem, as I see it, with some of the things that may not always be deemed sensitive. If the Supreme Court of Canada is saying that financial information is not always sensitive, perhaps we should listen to that.

Just to clarify a last point regarding paragraphs (f), (g) and (h), social security, passport and driver's licence numbers, passwords and financial data are not deemed sensitive in the GDPR or in Quebec's Law 25. Is that correct?

Ms. Runa Angus: That is correct.

Mr. Ryan Turnbull: Thank you.

[*Translation*]

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

Mr. Vis, the floor is yours.

[*English*]

Mr. Brad Vis (Mission—Matsqui—Fraser Canyon, CPC): Thank you, Mr. Chair.

I am very much enjoying what I think is a really relevant debate.

Going back to Royal Bank of Canada v. Trang in 2016, Mr. Schaan, could you please clarify if that case was ultimately about express consent or implied consent with respect to the sharing of information included in one's mortgage?

Mr. Mark Schaan: I'll turn to Ms. Angus to answer that question.

Ms. Runa Angus: That case was specifically about mortgage discharge statements and whether two banks could share a mortgage discharge statement with each other. What the Supreme Court decided is that they could because it wasn't sensitive information in that case.

Mr. Brad Vis: To my question, was it about an individual's relationship with the bank and having express consent to share that information, or did it establish a scenario of implied consent?

● (1145)

Ms. Runa Angus: I'll have to look at that and get back to you, because the crux of that case was specifically about the sensitivity of that information.

Mr. Brad Vis: All right. The way I understand that court case is that when the Trangs defaulted on their mortgage, they went to another bank and it said, “No, we can't share this information; it's sensitive.” However, the Supreme Court ruled they had given implied consent when they signed with the first bank and provided their personal information. Therefore, in the context of the sensitivity of information with respect to their mortgage, a bank was allowed to have access to that information because they provided implied consent when they signed up and got money from the bank in the first place.

I state that because I ultimately believe the argument being made by the department right now is factually incorrect. To state that you would have to provide express consent to buy an apple undermines a complete commercial relationship that exists already between every banking customer in Canada and the banks. Frankly, I think it's a bit of an irresponsible argument that's not well backed up.

I'll just make that point, and I say it with the most respect, because the interpretation bulletin on sensitive information—

Mr. Ryan Turnbull: It didn't sound respectful.

Mr. Brad Vis: I'm sorry; what's that, Mr. Turnbull?

Mr. Ryan Turnbull: I said it didn't sound respectful, but that's okay.

Mr. Brad Vis: Okay. Thank you for your opinion.

Mr. Ryan Turnbull: No problem.

Mr. Brad Vis: Under the interpretation, financial information is sensitive information. As the court in Trang notes, “financial information is one of the types of private information that falls at the heart of a person’s ‘biographical core’.... However, the degree of sensitivity of specific financial information is a contextual determination.” My understanding, based on the Privacy Commissioner's interpretation, is that you can still list information as sensitive and allow for a contextual argument to be made in the operationalization of the law.

What the department is saying right now is that they're predetermining the application and operationalization of sensitive information within the apple context that was provided today. I think that's a little over the top because we have well-defined processes in Canada between every banking customer and the bank that allow for sensitive information to be treated wisely. I don't see the basis of that...in addition to the nature of the Supreme Court ruling, which was about implied consent.

I'll ask you another question. In freedom of information in Canada, is financial information deemed sensitive or not under the freedom of information act?

Mr. Mark Schaan: Do you mean under the Access to Information Act?

Mr. Brad Vis: Yes, sorry, the Access to Information Act, section 20.

Mr. Mark Schaan: I'll have to refer to my colleagues, but to quickly go back to the previous point, there is no reading in of context in the proposed subamendment. It is a determinative list. It specifically states that sensitive information is this list. There is no paragraph that indicates “due to the context of its collection, use or disclosure”, for instance, which is what appears in the other versions of this, so there is no context and it is all financial information. It doesn't matter whether previously it would have been collected under implied consent or utilized thereafter with implied consent, because, essentially, by making it sensitive, we've required that it has express consent and it has express consent across every single aspect of the value chain.

Mr. Brad Vis: To push back, the Privacy Commissioner says, “However, the degree of sensitivity of specific financial information is a contextual determination.” He's stating there that financial information is sensitive, but it's also contextual. That's the point I'm trying to make, Mr. Schaan.

Mr. Mark Schaan: However, in the subamendment you've created, you're altering the rules by which he has the ability to interpret that, so there is no context. He's—

Mr. Brad Vis: We could state the whole thing about the applicability of PIPEDA in the context of a brand new piece of legislation. Maybe the courts are going to make a completely different determination because we have a brand new law. We haven't even gone into a debate about that and the application of some of the previous rulings the Privacy Commissioner has made and, by extension, maybe the Supreme Court will make one day.

● (1150)

Mr. Mark Schaan: To continue to highlight why the context.... The commissioner is only able to interpret that which is within the law, and right now, some of the proposals include a specific reference to context. This proposal does not. This proposal lists a set of information, decrees them sensitive and, because of other parts of the law, decrees that sensitive information requires express consent.

Mr. Brad Vis: What other parts of the bill?

Mr. Mark Schaan: The parts of the bill we'll get to, hopefully, lay out what the rules related to sensitive information are, including around consent. That's where it will state that sensitive information—or at least the current version says sensitive information—requires express consent.

Mr. Brad Vis: Can you point me to that section? I want to read it right now.

Mr. Samir Chhabra: I'm happy to add to that on behalf of Mr. Schaan.

Sensitive information is referenced in the bill in the definitions section, in proposed subsection 2(2); under “Privacy management program”, in proposed subsection 9(2); under the “Appropriate Purposes”—

Mr. Brad Vis: Can you just give me the page number, please?

Mr. Samir Chhabra: It's under, starting with the definitions, proposed subsection 2(2); under “Privacy management program”, in proposed subsection 9(2); in the “Appropriate Purposes” area, in proposed subsection 12(2); under “Consent”, in proposed subsection 15(5); under “Prospective business transaction”, in proposed subparagraph 22(1)(b)(ii); under “Completed business transaction”, in proposed subparagraph 22(3)(a)(ii); under “Retention and Disposal of Personal Information”, in proposed subsection 53(2); under “Security Safeguards”, in proposed subsection 57(1)—

Mr. Brad Vis: Mr. Chhabra, what specific section would apply to the apple example?

Mr. Samir Chhabra: I think the point Mr. Schaan was trying to make and the point we were trying to raise earlier—

Mr. Brad Vis: No, specifically, in the current bill, where would the interpretation of “sensitive information” be applied?

Mr. Samir Chhabra: The interpretation of “sensitive information”, of course, would be applied to all of these sections, but I—

Mr. Brad Vis: There are specific sections, though. I just want the specific number.

Mr. Samir Chhabra: Specifically, it would be consent. I think if I understand your example correctly—

Mr. Brad Vis: It's not my example. It's the department's example.

Mr. Samir Chhabra: I think it's proposed subsection 15(5) that speaks to consent.

Mr. Brad Vis: Thank you.

Mr. Samir Chhabra: I think the point the member was raising earlier was about how this would impact the practice. If I correctly understand the example reference made, there's already an existing payment system that would manage these issues. However, of course, the point the department is trying to raise here is that the payment processing system is predicated on our system of laws, including PIPEDA. In other words, PIPEDA, in the way that it's currently constructed, and the CPPA, in the way it was proposed to be put forward, enable these existing systems and processes when they are appropriate, lawful and rely on appropriate uses of consent.

The point that I think Mr. Schaan was raising earlier is that if we modify the definition of “sensitive information” in the way that's being proposed by the BQ subamendment, which the committee is considering right now, it would obviate the ability for those payment processing systems to rely on the current approaches they use. That's why it's particularly critical that we get the definition of “sensitive information” right.

I'll refer the committee back to the OPC's preferred formulation on this, which is to start with a reference to the notion that it depends on context. The context of the collection, use or disclosure is critical. Following that, we could put forward a list that is not exhaustive or exclusive and that gives an indication of the types of zones we're talking about. The current formulation of the BQ subamendment does not provide for the contextual analysis, nor does it provide any space for considerations of what could be on the list. It is, as Mr. Schaan already pointed out, a firm and final listing.

Mr. Brad Vis: One, it says, “but is not limited to”.

Mr. Ryan Turnbull: That just means you can add to it

Mr. Mark Schaan: What's on the list remains part of the list.

Mr. Samir Chhabra: In other words, the list itself is final. It can be added to, but what about the stuff that's on the list? The way this is currently constructed.... Our point is that it must be sensitive no matter the context.

Mr. Brad Vis: Going back to page 12 of the bill, under “Form of consent”, it ultimately makes the point I'm trying to make that we can have sensitive information and still allow for a contextual analysis, even though information is deemed sensitive. “Form of consent” on page 12 says:

> Consent must be expressly obtained unless, subject to subsection (6), it is appropriate to rely on an individual’s implied consent

I'm stating this in the context of the Supreme Court ruling that was referenced in the last two meetings, which was specifically about implied consent. It must take “into account the reasonable expectations of the individual”—which we haven't discussed, while we've taken a very black-and-white reading of what sensitive information would be—“and the sensitivity of the personal information that is to be collected, used or disclosed.” Later in the bill, what I'm reading is that there is a reasonable expectation built into information that could be deemed sensitive and its commercial applicability.

● (1155)

Mr. Samir Chhabra: Your reference to subsection 15(5) is what we're looking at too, and it says:

> the reasonable expectations of the individual and the sensitivity of the personal information

Both of those have to be considered in that scenario in order to be considered, so when you say “and the sensitivity”, and by definition you construct a bill that says that this information is always sensitive, you obviate the ability to take advantage of implied consent. You now default to a scenario of express consent, and that's the issue we're raising for consideration.

Mr. Brad Vis: Okay. I'm going to give that some thought.

Mr. Samir Chhabra: In other words, the test for appropriate use of implied consent requires two subordinate tests to be met: reasonable expectations and the sensitivity of the information. If we're automatically raising some personal information to the level of sensitive information at all times, it doesn't allow for this contextual analysis to occur.

Mr. Brad Vis: I don't completely agree with you, based on the interpretation bulletin from the Privacy Commissioner, but I'm going to leave it there.

Going back to my other question on freedom of information, it's my understanding that in the legislation in Canada, all information is deemed sensitive. The point I'm trying to make is that there are other contexts where financial information is deemed to be sensitive.

Here at committee, we've had to review contracts worth over $15 billion this year alone on Stellantis, NorthStar and Volkswagen. All of the arguments made about why the public shouldn't have access to that information were about it being sensitive information to the corporations. That's the context in which I'm approaching this. I know that's an example outside of the law, but it was really frustrating as an MP that we only had two hours with the contracts worth $15 billion.

Anyway, I digress.

Mr. Chhabra, that was a very helpful analysis. I still disagree, but you made a good point. Thank you.

[*Translation*]

The Chair: Thank you, Mr. Vis.

I will now give the floor to Mr. Williams.

[*English*]

Mr. Ryan Williams (Bay of Quinte, CPC): Thank you very much.

I agree that this has been a good discussion all around.

I think we may have to back it up a bit. When we look at the difference between personal information and sensitive information, the difference with sensitive information is that the potential harm or discrimination is greater. What we're doing is ensuring that there's an extra layer of protection when we're looking at these examples.

I'm one of the members who disagree with not having financial data on there. I think there's a higher degree of identity theft and fraud. It's the same with a driver's licence. Increasingly, through and through, we're seeing that Canadians are under threat of having their identity stolen. As technology gets better and we see Canadians using more apps and more technology, they're finding their privacy is under threat. I think listing these items as sensitive, especially when we see increased vulnerability from Canadians, is really important.

Mr. Schaan, where are we using “sensitive” in this bill as a whole? When we're talking about sensitive information, where are we using it generally?

Mr. Mark Schaan: I'll start, and then I'll turn to Mr. Chhabra.

As Mr. Chhabra noted, “sensitive” comes up in a number of places in the bill, the most important of which notes what you can't rely on as a use of information if the information is deemed sensitive, which is the example he just went through with Mr. Vis. We've cited a two-part test, essentially, for things like implied consent, and you can't rely on implied consent if the information is deemed sensitive, which means that it requires express consent.

Just to go back to last week's discussion, that's not to suggest that things like your driver's licence number or your personal information of a financial nature have zero protections. They have considerable protections, and by allowing, through guidance-making powers, the OPC to opine on these issues, you can get to effective oversight of that information without necessarily suggesting that in every instance, they require express consent, which is the most important part of what happens when you deem something sensitive.

I'll turn to Mr. Chhabra just to lay out again where “sensitive” comes up in the bill.

● (1200)

Mr. Ryan Williams: I'm sorry, but I'd like one more piece of context, Mr. Chhabra, when you're answering.

We use the word “generally” when we're identifying what's sensitive. Would the legalese for “generally” not imply that it's requiring an offer of acceptance or consideration without putting too much emphasis...? Are there ways that “generally”, used in this context, also allows a bit more flexibility?

Mr. Samir Chhabra: I would agree that the way it's formulated is intended to rely on the context-based assessment that would be undertaken. When you say something would “generally” be considered sensitive, you're giving an indication of direction. You're setting a policy framework parameter that allows for interpretation to occur effectively.

What is being contemplated before the committee now is to lock in a definition of “sensitivity” in the definitions section and then attempt to rely on it meaning generally sensitive. That becomes a law that is full of ambiguity and is very difficult to interpret and apply. It's not what the OPC has asked for, which is to have a context-specific determination with an indication, potentially, of some areas that could be considered sensitive.

To your earlier question on sensitive information, it's referenced 17 times in the act. I'm happy to reference each, if that would be helpful.

Mr. Ryan Williams: It's not in the definition, but it is implied that this has a greater potential for harm and discrimination against individuals. We've looked at this whole bill from the outset, and it's not yet in the purpose statement that privacy is a fundamental right.

We're looking around the corner, and I'm looking to add an amendment. I'm going to add one piece that isn't in here that I think is really important, given where technology is going to be in the next 10 years or so, which is on location data. When we look at that piece of information, location data is everything we have on our phones, our watches and our cars that identifies who we are and where we are.

Going backwards on that, when we look at financial data, it is also evolving. We have open banking in front of the government right now. We've been pushing for that. Open banking is about ensuring that customers have control of their financial data with their consent. That's very much the wording of what we've listed. Customers then have control of that.

If it's not sensitive data, then what are we doing with consent and how we're giving it? I think it's a form of control for Canadians and for people that, when we're looking at privacy as a fundamental right, it is listed most of the time that on your consent, you can move your information somewhere. If your data is being recorded and tracked, it has to be with your consent. To me, that, by its very nature, when it comes to harm or discrimination, is sensitive. Further along in the bill—because we're only on the definitions side of this—we can take that context and debate how that's used or what's going to happen. However, I don't think we should be taking that out of what we deem to be sensitive.

If we go to the potential for harm or discrimination, obviously we're looking at an extra layer of protection for security PIAs, but I think we're really, as a committee, just defining information that is exceedingly being used in identity theft, fraud, stigmatization and discrimination. I think all we're doing is listing that as something we want to protect, and I think what we've been trying to identify are those things.

Mr. Chair, I'm going to talk about it first, but I'd like to add paragraph (i), which would be location data. I'll note why that's important really quickly.

Location data is considered sensitive for several reasons. We have personal security and safety. Location data can reveal where a person lives, works and frequently travels—

Mr. Ryan Turnbull: I have a point of order.

I'm sorry to interrupt you, Mr. Williams.

Mr. Ryan Williams: I don't think we have a chair for the point of order.

We can take a recess, Mr. Chair. What is the soup today?

The Chair: I was inspired by Mr. Perkins.

Mr. Turnbull, go ahead on the point of order.

Mr. Ryan Turnbull: I just wanted to check whether you can introduce an amendment to a subamendment. I don't think you can. I think Mr. Williams is sub-subamending something, which is not procedurally correct.

● (1205)

The Chair: That is correct, Mr. Turnbull; you can't amend a subamendment. We are now debating a subamendment.

Mr. Williams, perhaps, should this subamendment by Mr. Garon be passed, you can amend the amended amendment.

Mr. Ryan Williams: Yes, okay. Then I will summarize it.

I'm not making the amendment now, but in relation to my argument about sensitive data, location data is certainly an addition. Going back to my original argument on this, I think when it comes to what we're looking at for consent, this is not the section in which to debate that. I think we're debating what is sensitive data, what can be used for potential harm or discrimination and what needs an extra layer of protection. Certainly, I think the items that have been listed are all part of that, and I believe that Mr. Garon's subamendment is a good one.

[*Translation*]

The Chair: Thank you, Mr. Williams.

Mr. Masse, you have the floor.

[*English*]

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

I think it's important to note we're at an impasse. There's a philosophical argument here more than a technical one with regard to the bill. For me, the use of data in the system that financial institutions currently employ is inefficient for the economy. It is certainly to the disadvantage of the consumer, and that's one of the things I'm looking to change with this bill.

I joked about automobiles when Mr. Williams mentioned some of the location issues that he referenced. He's actually very astute in saying that, because the value of automobiles in the future will be as much about gathering information as it will be about producing, manufacturing and distributing them back into society. It's going to be about the value of the consumer, who needs to have some choice.

This rights a social injustice and an economic dependence model we have when it comes to financial institutions. That basically puts consumers and small and medium-sized businesses at a disadvantage in our economy. It's pretty abhorrent that some of the information gathered right now by credit card companies is routinely distributed and sold to give a financial institution leverage to use against its own customers.

What I want to see this amendment do, from where I'm standing at this point in time, is strengthen the path forward so people have a calculated ability to use their information to quantify that, even economically if they want, by consent. I think some of the fear coming out of this is that if you do anything on your phone, you're going to be crippled, because we've gone ahead with this type of amendment. However, it can be quantified so that if you, for example, want to sell or give access to your information in an empowerment model, it can be for reduced fees and costs or for financial incentives, which could be granted to you through the changed system of information.

I don't really have a question at this point in time. I'm not sure how far the government wants to go down this road if they don't have support from other parties for their particular position. I understand where it comes from. I understand some of the arguments that have been made. It really comes down to a determination of how long they want to prolong this bill and prolong this process, because I'm not moving off the spot. It's of definite benefit to the social and working class to have empowerment models for their financial information and otherwise. It's up to businesses to come forward with a model that works for them. It comes at the expense of having better supports for the consumers and supporting their customers.

Where we go at this point, I'm not sure. I think there's a philosophical impasse at the moment, and we can continue to have more questions and comments. However, I would like to see the privacy component of this bill move quickly. At the same time, I'm looking for a philosophical change. That's where the NDP is at this moment. We're using the leverage we have at this point in time as an opportunity to turn the financial institutions back to where they should have been historically, which is serving customers. Information is everything in this day and age, so taking more opportunities to leverage it for the working class is what we should be doing, because the fees, the costs and the financial way this country has been endorsing these policies are very inefficient for productivity.

I'll conclude with that because it's very important to understand that our money management and information systems are very much tied at the hip. Why would we undermine consumers or individuals being able to exercise their rights? That would be a mistake.

● (1210)

[*Translation*]

The Chair: Thank you.

Mr. Garon, you have the floor.

Mr. Jean-Denis Garon: Thank you, Mr. Chair.

Many things have been said about this amendment.

First, the government doesn't want it. The government doesn't want our extremely sensitive financial data, which can be stolen and used, subjected to a fairly high level of consent.

It's deplorable. I can't repeat it enough. We don't know who the minister consulted before tabling Bill C-27, which ended up generating a ton of amendments because it was poorly drafted in the first place.

We don't even know which banks, which financial institutions, which insurance companies or which private interest groups were consulted. Perhaps consumer groups were involved. We don't know. However, clearly, if we're to again believe the advocates of this bill, we seem to be hearing from people in the industry.

My subamendment has been worded to include the contextual component. When we say that "the individual generally has a high expectation of privacy", this implies that the Privacy Commissioner can incorporate the contextual component. There's absolutely no ambiguity here.

In Quebec, Law 25 provides some protection for financial data. However, we would like to remind the government that most financial institutions are federally regulated.

Mr. Chair, I would like to share the following quote from a Supreme Court ruling: "… I agree with the Privacy Commissioner that financial information is generally extremely sensitive." I repeat: "… I agree with the Privacy Commissioner that financial information is generally extremely sensitive."

This ruling is found in the Trang case. The Supreme Court recognizes that, in some circumstances and business relationships, a certain amount of consent is implied and the courts have leeway when it comes to interpreting that consent.

My subamendment doesn't say that financial information is always sensitive. Nevertheless, generally speaking, that's what it says for cases where the circumstances point to a high expectation. This fully aligns with the Supreme Court ruling in the Trang case. The subamendment was written with this in mind.

I also really want to emphasize that I share my colleague Mr. Masse's view that not including financial information would mean a step backwards from current law.

Once again, we stand by our position.

I also want to quickly address the comments made by my colleague, Mr. Williams.

We're saying that sensitive information isn't limited to the information on the list. Geolocation data is an example of information that could be considered sensitive, if the individual generally has a high expectation of privacy in this area and if the information is read in context.

This shows the importance of providing a certain amount of leeway given that five-year reviews don't always take place after five years. In some cases, they take place after 8, 10 or 12 years.

I think that the amendment should be passed.

Lastly, consent fatigue must be taken into account. We're told that people will become tired of having to consent to the use of their information. Given this sociological phenomenon, we should refrain from including a person's financial information in their sensitive information.

I have no doubt about the scientific training of the officials here today. However, I took the liberty of consulting the scientific literature to find out about consent fatigue. That's what I read.

I understand that people may ultimately become tired of having to give their consent when alerts pop up every five seconds on their Apple watch—like my colleague Mr. Turnbull's watch—each time a bank wants to use their personal information.

However, apart from the office of the Minister of Innovation, Science and Industry, the fact remains that no one is currently talking to us about consent fatigue.

People are afraid that their data will be stolen and used.

● (1215)

People are afraid of being located. We know that devices, especially cell phones, contain a great deal of information. People talk to us about it. However, I have never heard anyone ask me to be careful that we don't wear them out when we legislate to protect their personal information. That has never happened to me. I don't accept that argument.

The Chair: Thank you, Mr. Garon.

Mr. Turnbull, you have the floor.

[*English*]

Mr. Ryan Turnbull: I'm hearing out all my colleagues here, but I really feel like this is going to have a negative impact. The officials have said to us numerous times when I've asked them questions that this subamendment deems everything on that list, even though you can add to the list, as sensitive, and therefore requires express consent every time the data is collected, used or disclosed. Just imagine the impact that might have.

This is not to argue against the points that have been made. Ideologically, yes, I agree. All of the information is important information that needs to be protected and should come with some pretty stringent requirements. That's part of the construction of this bill, as I understand it. That doesn't mean that every single piece of personal data should be deemed sensitive. I know that's a bit of an overstatement, but I think we've argued numerous times that this list includes things that are not in the EU's GDPR.

I have the EU's GDPR right here. I'll give you the very specific information that's included in it. I'm surprised that members are arguing that this list is included in the GDPR. It's not, as far as I can tell. When I type in what personal data is considered sensitive in the EU's GDPR, it lists this:

> ...personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation....

That's it.

I also understand, from asking officials, that the list that's here.... We have paragraphs (f), (g) and (h), and Mr. Williams wants to add (i), which is location data, if we ever get to that point. I would argue that this list would put us out of alignment with both the EU and Quebec's Law 25.

Can I clarify that, Mr. Schaan, and get you to state that again? Is it the case that we would be out of alignment if we had all of paragraphs (f), (g) and (h)? If they're included successfully and this subamendment gets passed, that will put us out of alignment. In other words, Canada would have a law that is more stringent than Quebec when it comes to deeming personal information sensitive. Is that correct?

Mr. Mark Schaan: By the drafting of the list currently and including these broad concepts, yes, it would extend well beyond what is currently deemed sensitive under both Quebec's law and the GDPR.

Mr. Ryan Turnbull: Would this harm commerce in the country? Would this have a really harmful impact on the general flow of commerce? We walk into grocery stores. We buy things. We use our Interac cards all over the place.

What impact would this have on the average Canadian? I think it would have a pretty significant impact.

Mr. Mark Schaan: I'll let my colleagues weigh in as well.

The value chain for the processing of financial information in particular is a multi-stage value chain. It involves multiple players outside the initial collector because there are people in the value chain for financial services who do very different things.

There's the initial piece about the payment, transaction and point of sale, which potentially collects the initial information. It then needs to continue along the value chain to ultimately allow the funds to come out of your bank account and get paid to the people who are supposed to receive them. By suggesting that this is generally sensitive information, it will require express consent, which means that you need to expressly consent for every single step along that value chain, because each one of those things is considered a disclosure. At minimum, that upends a significant number of current business processes, but it will create a significant amount of responsibility for the individual to allow for the movement of their financial data and allow for the continued fulfillment of their economic needs.

I'll turn to the team to see if they want to add anything.

● (1220)

Mr. Samir Chhabra: Just briefly, to echo what Mr. Schaan said and amplify it a bit, you can think about this in terms of the impacts that it will have on commerce on a day-to-day basis. You can also think about it in the context of interoperability of systems. A big discussion at this committee over several different meetings was about the degree to which Canadian businesses are incentivized, the degree to which the competition framework drives innovation and the delivery of new and effective services, and the degree to which our systems are able to attract investment.

I believe committee members this morning referenced open banking or consumer-driven banking, which is an ecosystem that relies entirely on data-driven innovation to create new competitors and to shake up the legacy system. In that context, having a different rule set or approach to the sensitivity of information could have an impact on the degree of investment attraction and the new services and offerings that are developed and put on the market. Again, an important piece to consider is whether there's actually a significant enough value-add from adding financial data to outweigh those other considerations.

Mr. Ryan Turnbull: Is this what the OPC asked for? It sounds to me like the Privacy Commissioner is not asking for this particular approach. The Privacy Commissioner wants some categories of sensitive information to be identified, but wants to be able to use discretion and consider context in identifying how sensitive certain personal information is. Is that not correct? What would the Privacy Commissioner say about this particular subamendment if he were here today?

The Chair: Before we get to an answer, Mr. Turnbull, I'd appreciate it, colleagues, if you waited until the end of the meeting to have discussions, or you can ask for the chair to suspend the meeting. Out of respect, please, I ask everyone to listen to the discussion we're having. It's an important one.

Go ahead, Mr. Schaan.

Mr. Mark Schaan: The commissioner indicated in previous fora that he believes it's important that we have a definition of "sensitive", that it list the categories that are likely to be sensitive and that it include context for collection, use or disclosure to allow for context to be laid out through his guidance. The categories that he's listed do not include those that are currently in paragraphs (f) through (i).

I'll turn to my colleagues to further confirm that.

Mr. Samir Chhabra: Thank you for that.

The commissioner has been clear about the interest in having a context-based definition as the foundation for any definition that the committee chooses to adopt. I also think it's worth pointing out that the commissioner issued guidance on this issue several times, including most recently in 2022.

For greater certainty about what we're talking about here, it should be really clear that not including something in this list as part of the definition does not obviate the commissioner's ability to include it and to provide a much more detailed context-based definition or parameters around what will make certain types of information sensitive in a given context, including many types of financial information, which can also be included via OPC guidance. I think the issue before the committee right now is about whether the unintended impacts that could occur by listing an item strictly in the definitions will be worth the effort to do so. The consideration is what that offers over and above what the commissioner is able to do via guidance.

● (1225)

Mr. Ryan Turnbull: Mr. Garon has said that, potentially, consent fatigue is not really a thing. I think if we make this a subamendment, it will become a thing. It will become a much bigger issue for the average Canadian. I trust that the systems we have in place are protective, and I understand that sometimes they break down. Sometimes there are breaches of privacy. Those are things that the Privacy Commissioner will be able to deal with.

Are there aspects of this bill that we haven't contemplated yet that can assure the members of this committee that certain types of information included in paragraphs (f), (g) and (h) are protected but not necessarily always deemed sensitive? I think that's the heart of the issue for me. I hear ideological arguments about protecting information that members want to deem "sensitive" to ensure that it's held close and really protected.

I get the desire to do that. I get the motivation behind it. There's a good motivation behind it. However, think about the ramifications or the unintended consequences of that when not being able to consider context. I think that's really the issue. Also, the bill itself is designing a framework to ensure that paragraphs (f), (g) and (h) still come with requirements that are significantly robust and perhaps more robust than in the past.

Mr. Schaan, can you speak to that? I ask because I feel like this is the missing piece. We're stuck on a definition. We're trying to do something in the definition that the rest of the bill will deal with in due course, but we haven't gotten there yet. I don't mean this in a disparaging way at all, but we're not there yet in the bill. We haven't looked ahead and necessarily gotten to that point.

Mr. Schaan, can you give us some detail on how the bill, in later phases or stages, raises the bar and the requirements for personal information and suggests that not all of it needs to be deemed sensitive for it to be protected?

Mr. Mark Schaan: That's right. The overall structure of the consumer privacy protection act makes significant improvements to the existing Personal Information Protection and Electronic Documents Act in the treatment of both personal information generally and sensitive information. Some of what would be wrapped up in requiring express consent at this point will be further contemplated. For instance, what are the obligations for the general protection of personal information? What sorts of privacy programs do you need in place to ensure that you've done things like having effective controls? Have you left yourself vulnerable to cyber-risks or other aspects, for instance? Those are the sorts of things that will get covered in a privacy program.

There will also be further considerations about what it takes, and when you are allowed, to make a disclosure. When am I allowed to move financial data, for instance, from one payment process to another, and what are the guardrails around that?

There will be, as contemplated in the act, a very high standard set for the treatment of personal information writ large, including in a number of the instances that would get wrapped up in what it currently contemplates and tries to do through sensitive information. By making it sensitive, we are requiring its express consent, therefore taking away the flexibility of the context-specific reading that the Privacy Commissioner has asked for. It also suggests that all of the other things that will come later that protect that information won't be doing anything, when in fact they very much will.

I don't know if my colleagues want to weigh in.

Mr. Ryan Turnbull: I'm looking for the specific section that deals with personal information and the requirements around it that would perhaps reassure committee members. I'm struggling to find it in my binder, but I know I've read it and can definitely find it.

Mr. Mark Schaan: I'll turn to the team. They can point to some sections that deal with the treatment of personal information and the important guardrails around it.

Mr. Samir Chhabra: As I mentioned earlier, there are 17 instances where sensitive information is specifically mentioned, including in proposed subsection 15(5), which talks about the form of consent. It appears under “Retention and Disposal of Personal Information”, in proposed subsection 53(2). It also appears under “Security Safeguards”, in proposed subsection 57(1), and again in proposed paragraph 58(8)(a).

It's really throughout the entire act. If we're looking for areas of the act that speak to the responsibilities and accountabilities of data holders, it is quite well spread out.

My colleague might have a few other references for you.

● (1230)

Ms. Runa Angus: We have to remember that when we talk about personal information writ large, it's not just about sensitive information. All the obligations, whether about security safeguards or about retention and disposal, as my colleague said, are applied to all personal information. It's the degree that changes.

With respect to any personal information, there is obviously the appropriate purpose. You can't collect, use or disclose any personal information unless you have an appropriate purpose for doing so, and that's an obligation that applies to all personal information, not just sensitive personal information. You can't use information just because you want to. That's an obligation that applies in all contexts.

Mr. Ryan Turnbull: Okay. Thank you.

I know that members opposite have mentioned open banking. What impact would this subamendment have on open banking? It seems to me that it would have a pretty big impact on the possibility of moving forward with an open banking system.

Mr. Mark Schaan: I'll start. Then my colleagues will likely want to weigh in.

As noted, because financial data will now be deemed sensitive information, consumer-directed financing, as it's understood, will rely on the data portability obligations that are found within later sections of the CPPA, which would have a direct one-service provider for consumers to provide their information to another service provider. However, that doesn't obviate or shift away the realities of the financial services sector that then would follow.

That new fintech player is probably more reliant than others on third party processors or other aspects, because they've made their niche in one aspect of financial innovation, which is potentially providing services, but that doesn't mean they're going to have the whole back end that would normally be accompanied by a larger financial services provider. Every single one of those disclosures will require the express consent of their client, which means that when they want to provide a seamless financial services environment for their client, they will be going back to their client on numerous occasions to reseek their consent for the continued disclosure of financial information.

I don't know if Samir and Runa want to weigh in.

Mr. Samir Chhabra: I'll add to that.

Having had the opportunity to speak to some of the experts in the open banking or consumer-driven banking space in recent days, I'm comfortable sharing that when considering specific issues related to consent, authorization and authentication—which are each different steps in the value chain that all need to be appropriately managed for different purposes within the consumer-driven banking system—insisting that all financial data become sensitive information changes the calibration of the work that's under way there. I think it would be entirely reasonable to say that it's likely to slow down the advancement of the work that's currently being contemplated. There's an important distinction to be made between express consent when sensitive or personal information is being managed and elements that, while still being designated as personal information, may not attract a level of sensitivity given the context of the use or disclosure that's being made to enable open banking, which in some cases is about transferring information to enable services to be provided.

The point here is that's it's a bit like an iceberg. We need to understand that express consent is visible and available to all of us as consumers in the system, but there's a lot of work that needs to go on in the plumbing, if you will, to share data that wouldn't be sensitive given the context, in order to enable the provision of services that we see at the consumer level.

Mr. Ryan Turnbull: Is some financial information always sensitive? Is there an argument there? I'm playing devil's advocate. Is there some portion of all financial information that should always be deemed sensitive? If not, then this is really problematic.

It's even more problematic than I initially thought, but is there a way to determine that a category of financial information would always be deemed sensitive without considering context, or does context always matter? I know it's a difficult question, but I thought I'd put it to the officials anyway.

● (1235)

Mr. Mark Schaan: I think there's a lot of financial data that many of us would be uncomfortable seeing shared outside of those we know, but context does matter. I could ask you if you're you okay with me knowing how much you have left on your mortgage or how much your monthly mortgage payment is. You would probably not want a wide body of people to know that. However, let's say I told you that when paying your mortgage, when you send the transfer—either automatically or, if you have to do it manually, through your electronic banking app—it was going to pass through six different processors to ultimately move from the part of the bank that has your savings account to the part of the bank that holds your mortgage, assuming that's even in the same financial institution. If I told you that it was going to pass through six or eight hands and asked, as it's probably pretty sensitive, “Do you want to make sure that you know about every single one of them?”.... I think if people knew that those disclosures were managed by a privacy program where there needed to be a clear rationale for why that information was being shared, and knew that the original collector was still ultimately accountable for its treatment and the privacy obligations throughout the entirety of the value chain, many people would say they're comfortable, they don't want say yes eight times and they want that information just to flow.

I think that's what makes it so tricky to say that in all instances this information is always sensitive, because in many cases it's not sensitive within a given context.

Mr. Ryan Turnbull: If I were to summarize what you've said, it's that context always matters with regard to financial data. Is that not the underlying point you've made with your example?

Mr. Mark Schaan: I think that's fair.

Mr. Ryan Turnbull: Would the seamless financial services environment that you described be a thing of the past if this subamendment passes?

Mr. Mark Schaan: The business processes that I understand are currently in operation in the financial services sector have multiple players within them requiring multiple disclosures per transaction, and if each one of those disclosures is subject to express consent, that would be a very different financial services experience than what we have currently.

Mr. Ryan Turnbull: I'm glad to hear you didn't use the apple example. I noticed that triggered my colleague Mr. Vis earlier.

Mr. Brad Vis: It did.

Mr. Ryan Turnbull: Thanks for the clarifications. We appreciate it.

[*Translation*]

The Chair: Thank you, Mr. Turnbull.

Mr. Perkins, you have the floor.

[*English*]

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

Thank you, officials.

Before I ask a couple questions on this, which I don't believe I've talked to yet, I note that this is the third meeting we've had on CPC-7, most of which has been driven by the government's desire to amend and change it. I note this only because the government suggested that clause-by-clause would take four meetings and the government is the one pushing to make it longer.

Mr. Schaan, I'm a little concerned by your testimony earlier about the Privacy Commissioner. Bill C-11, which was the predecessor to this bill, attempted to make Privacy Act changes in the last Parliament, and I would like to read from the Privacy Commissioner's submission on it to committee, if I could:

> While the OPC and the courts have provided some interpretations of sensitive information, it would be preferable to have a legislative definition that sets out a general principle and is context-specific, followed by an explicitly non-exhaustive list of examples (such as those included in article 9 of the GDPR). This would provide greater certainty for organizations and consumers as to the interpretation of the term. For instance, such a definition might read:
>
> Sensitive information means personal information for which an individual has a heightened expectation of privacy, or for which collection, use or disclosure creates a heightened risk of harm to the individual. This may include, but is not limited to—

Does that sound familiar? It's in MP Garon's subamendment.

> —information revealing racial or ethnic origin, gender identity, sexual orientation, political opinions, or religious or philosophical beliefs; genetic information; biometric information for the purpose of uniquely identifying an individual; financial information; information concerning health; or information revealing an individual's geolocation.

That was for the last bill, so it comes as a surprise to me, Mr. Schaan, that you said the Privacy Commissioner has not asked for that. It's right in his brief.

● (1240)

Mr. Mark Schaan: Mr. Perkins, I would note that Bill C-11 was contemplated by a previous Privacy Commissioner.

Mr. Rick Perkins: Oh, okay. Then it doesn't matter that the Office of the Privacy Commissioner said that.

Let me go forward. Are you aware of the California privacy law?

Mr. Mark Schaan: Yes, I am.

Mr. Rick Perkins: You're aware that the particular clauses that irritate the government are actually in that law.

Mr. Mark Schaan: I'll turn to Mr. Chhabra to talk about the California consideration.

Mr. Samir Chhabra: I think it's really important to point out that the testimony being referenced speaks to the interest of having an example provided in the definition.

I want to make it clear that what we're reacting to in front of us with the amendment does not provide examples. It doesn't say "may include", for example. It says "includes". That's entirely different from offering a context-dependent definition followed by some indicative examples. In that way, it's completely different from what we're contemplating here.

Mr. Rick Perkins: I can tell you, as a guy who worked for five years at the head office of a Canadian bank and sat in focus group meetings with individuals and customers, that many customers don't even share their information with their spouse. Believe me, financial and health information are among the most sensitive information, and people want protection.

In addition, are you aware that in the United States there is the American data privacy and protection act going through Congress, which does exactly this? It's a bipartisan bill.

Mr. Mark Schaan: I'll turn to Mr. Chhabra, but I'll note that one of the fundamental aspects we've tried to draw out over the course of the discussion today is the importance of some sort of context-specific interpretation tool at the outset of the list. It's something that would read like, "due to the context of its collection, use or disclosure, an individual has a high expectation of privacy and may include". One aspect is context. The second is whether that's deemed to include, by definition, all component members of a class of information or it's indicative.

Those are two very important points that we're getting at. I think in the current formulation, there isn't the same understanding of the context of collection, use or disclosure, and the list can be added to, but is definitive in its contents.

Mr. Rick Perkins: Have the California law and the GDPR law meant that every time somebody uses a debit card they're required to provide permission?

Mr. Mark Schaan: As noted, the GDPR does not include financial data as sensitive information.

Mr. Rick Perkins: California does, and they have more population than all of Canada.

Are they asking, every time they use a debit card, for permission?

Mr. Mark Schaan: Mr. Chhabra may be able to speak to the specific formulation of the California law.

Ms. Runa Angus: California does include financial information as sensitive information, but as for whether that means that when you use a debit card you need express consent, it's you using the debit card, so I don't think.... By using the debit card, you're consenting to it.

Mr. Mark Schaan: Our previous point was about the processing of that information. I don't know the formulation of the California law well enough to know whether it also includes an obligation for express consent and whether disclosures are wrapped up in that.

Mr. Rick Perkins: Mr. Schaan, the current Privacy Commissioner, in the appendix to his submission on Bill C-27, also asks for the list.

Mr. Mark Schaan: He notes the importance of context and he notes an indicative list.

● (1245)

Mr. Rick Perkins: The government believes in the right of a large financial institution, as an example, to use your personal financial information in a way that isn't considered sensitive. That's the side it wants to be on, not the protection of an individual's privacy and the requirement for permission, which they can get as a blanket permission. It's not a difficult thing. We all give blanket permissions for privacy and the use of data when we subscribe to banking services.

Mr. Mark Schaan: I would be uncomfortable with that characterization. I suggest that the government is suggesting the definition of sensitive information should have important flexibilities to both understand context and understand cases and use cases where that information may not be sensitive.

I would note that we are not suggesting the personal information protections afforded to non-sensitive personal information should ever result in a violation of someone's privacy or affect their fundamental right to privacy. I think that's comparing two very different things.

Mr. Rick Perkins: I'd argue that, by the time this bill passes, we'll already be out of step with California and we'll be out of step with the United States, given where they're going with regard to the American data privacy and protection act.

That's it for my questions, Mr. Chair.

[*Translation*]

The Chair: Thank you, Mr. Perkins.

Mr. Généreux, you have the floor.

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

I want to thank the witnesses for joining us.

While we were debating these issues, an article came out on TVA Nouvelles. This article reports that Hyundai was hit by a data leak and that there has been a 225% increase in this type of leak since last year.

Our colleague from the NDP spoke about the information that cars collect. I'm happy to still be driving around in a 2009 car. No one knows where I'm headed with this car. That's reassuring.

Mr. Turnbull is concerned that, if amendment CPC-7 were passed, as amended by the subamendment, people would be required to give consent at every stage of a value chain process.

Legislation is implemented by regulation once it has been passed. Can these regulations be drafted in a way that avoids multiple authorization requests at each stage?

Mr. Mark Schaan: It isn't about regulations. It's a definition that includes sensitive information. It's about interpreting the definition.

Mr. Bernard Généreux: Let me remind you that the government has moved 50 amendments to the bill, and that a number of subamendments must be reviewed. Obviously, the bill is full of flaws, to say the least, and we're trying to correct them.

If we add a list of these types of items, even a non-exhaustive list that allows for possible interpretation, will these items be implemented by regulation, thereby providing the leeway needed to implement the bill?

Mr. Mark Schaan: In this case, it's hard to predict the possible interpretation given the construction of the sentence. It says that the list is non-exclusive. However, all the items on the list are included in the definition. There isn't any room for interpretation, because it's clear.

As a result, we find that the commissioner should be given some context at the start of the list, and that the list should be indicative.

● (1250)

Mr. Bernard Généreux: I gather that you don't want the CPC-7 amendment at all, and that you don't want a list.

Is that right?

Mr. Mark Schaan: No. We're comfortable with the idea of including a list, but an indicative and non-exclusive list.

[*English*]

The list needs to have both aspects so that there can be more than what's on the list and so that what's within the list is indicative, thereby giving context to the Office of the Privacy Commissioner. Then it can indicate the context in which information would and would not be understood to be sensitive.

[*Translation*]

Mr. Bernard Généreux: Thank you.

The Chair: Thank you, Mr. Généreux.

Mr. Williams, you have the floor.

[*English*]

Mr. Ryan Williams: Thank you.

I want to touch on the financial aspects we've been talking about, specifically open banking. Strong data protection is a selling point for open banking. That's why it's being looked at for Canada. It's allowing better data protection technology to come into effect.

Mr. Chhabra, you've spent some time talking about open banking. I've spent thousands of hours talking to individuals on that and trying to push forward...specifically because they believe the API and the framework that's going to be developed are going to make them more competitive against standard banks in the whole process. We've seen that in Australia and the U.K.

You indicated that you already talked to some of these groups. I'm still unclear as to how listing financial data as sensitive is going to hurt our financial institutions in Canada. I think it's going to strengthen them. If there is increased consumer protection and technology that will protect that data, and if we are ensuring that consumers of Canadian technology in Canada are going to have greater protection of that data, I'm not sure why we would see that as a disadvantage, specifically since up to now the only thing that's been produced in the budget is to grant the framework for open banking, with more consultation with the industry.

If we're developing an API that's going to be used across the whole spectrum in open banking, why would this put our open banking system and framework at a disadvantage compared to those of other countries?

Mr. Mark Schaan: It's about disclosures. It's about the nature of requiring express consent for every use, collection and disclosure of financial information, because the list as constructed says that such information is, by definition, sensitive, which means it cannot rely on implied consent.

Therefore, the processing of financial information, which is often transferred from one collector into the hands of another as part of an accountability chain, will require the express consent of the individual. Each one of those steps puts at a disadvantage the notion of a convenient framework that tries to preserve consent for where it is most important, which is when the privacy of information is potentially at great risk and when information is potentially not understood, in the capacity of an individual, to be transferrable as part of the service they're receiving.

Mr. Ryan Williams: Okay. This will be my last comment, and hopefully we'll get to a vote on this shortly.

I think what that framework does, when we look at the financial sector and open banking, is it allows customers to explicitly grant or revoke consent and makes third party access easier than any other framework we've had in the past. Open banking should be the example of why we're including financial data as sensitive and why Canada wants to protect that data explicitly. As to the second part, we've included “generally” because that word gives flexibility to the Privacy Commissioner to then deem what financial data can be used, given the sensitivity of it, and in what context it should be used.

I think we've given all of that and we've gone around the room on this quite heavily.

Thank you, Mr. Chair.

[*Translation*]

The Chair: Thank you.

Mr. Masse, you have the floor.

[*English*]

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

I want to get on the record some of the differences we have.

Here we're talking about the empowerment of consumers with regard to information, but at the same time, we have a government that has not moved on Crown copyright since 1911. For those who aren't familiar with Crown copyright, it was first brought to Canada in 1909 and was amended in 1911. What that means, which is really important to businesses, educators and general society, is that all the information the government has is basically suspended or not provided to the public. That is different from what our U.S. counterparts and other Commonwealth nations have. I find it difficult when the government wants to continue to have control of publicly manufactured and basically publicly expensed information when the United States doesn't do this, Great Britain doesn't do this and the other Commonwealth nations haven't done this.

Mr. Schaan, with regard to Crown copyright, what country out there is equivalent to ours? The argument is being made that the government wants to defeat this amendment to allow the public to have information and control. At the same time, this government continues to block Crown copyright renewal, which is actually providing information to the general public that they've paid for. Where in the world is there a consistency of Crown copyright?

● (1255)

Mr. Mark Schaan: As it relates to the government's position on Crown copyright, it's not a singular position. I think it's important to look at the Treasury Board guidance that relates to the publicity of information generated by the Crown, including the open-by-default standard and the importance of ensuring that information is actually openly shared. There are a number of particular uses of copyrighted information on the Crown side that need to be understood in their full context.

Mr. Brian Masse: Is there a country you can think of that has a regime similar to ours? Can you give us an example of another country?

Mr. Mark Schaan: I'm not sufficiently familiar, as this hearing today is on the privacy bill, with the full international examples of Crown copyright.

Mr. Brian Masse: I appreciate that, but it goes back to the importance of why information is deemed valuable. At this time, we still don't have any comparables.

I'll leave it there, my point being that I find it highly ironic that the government values its information manufactured through public expenses—which would be very beneficial to businesses and academic research—but, because it has control of that information, is not releasing it. Even the former parliamentary secretary for the Liberals in this position, the former solicitor general, was much more open to and was pro the reform of Crown copyright, but we know what happened with that situation.

Thank you, Mr. Chair.

The Chair: Thank you, Mr. Masse.

I have MP Van Bynen and then MP Turnbull.

Mr. Tony Van Bynen (Newmarket—Aurora, Lib.): Thank you, Mr. Chair.

It seems to me that the concern here is around privacy of information and the sensitivity of information.

Mr. Schaan, could you just clarify for me what types of protections contained in this legislation address the privacy of information?

Mr. Mark Schaan: There are a number of provisions we have yet to get to in the CPPA that heighten the level of privacy protection for all personal information collected, used and disclosed by corporate entities in the Canadian context. They include requirements for express consent in a number of areas, as well as limitations on when and how other forms of consent can be relied upon. The CPPA also puts in place a very significant enforcement regime over the uses of both those exceptions, as well as the privacy protection programs that need to be in place. For instance, there's the scrutiny of the security measures that a company must put in place to ensure they're not exposed to breaches or vulnerabilities. There's the enforcement of exceptions. Where an exception to consent, if it's relied upon, is found by the Privacy Commissioner to not have been reasonable, it's moved into an unlawful usage of personal information, which means that it's subject to the most significant fines under the administrative monetary penalties regime.

It's a very robust overall approach to the treatment of personal information, of which sensitive information is a subset that has a heightened level of privacy protections. However, the one that's the most important for this conversation is express consent.

Mr. Tony Van Bynen: You mentioned earlier that certain obligations are required to maintain privacy. Can you expand on that, please, and on what the implications are in relation to what's being discussed? Specifically, I'm concerned about the differentiation between “sensitive” and “private”, but more importantly, what kinds of obligations are there to maintain the privacy of the consumer and what's the Privacy Commissioner's role in ensuring that's being done?

● (1300)

Mr. Mark Schaan: The entire regime is overseen by the Privacy Commissioner, who has considerable capacity, such as the power to make orders and recommend AMPs and the ability to enter into consent agreements to modify the behaviour of those who potentially violate the privacy of Canadians. All of this is interpreted within the broad category of a fundamental right to privacy, which was inserted in the preamble and at the outset of the bill.

The personal information use cases that we've talked about today would be governed by strict obligations for the use of personal information, notwithstanding that it's not sensitive. A company would need to be plain-language clear at the point of collection about what the uses of the information were and what the individual could likely expect for the ongoing transfer of that information. They'd need to have a privacy program in place that would include the safety and security of the information in their disclosures.

Those obligations would pass on to a disclosed entity. If a disclosed entity is a payment processor in this particular use case, notwithstanding the fact that this doesn't obviate the accountability of the original collector, they are required to continue to ensure the trust and security of the information in their possession, notwithstanding that it was transferred to them without express consent.

Each step in that value chain is still governed by an overall approach that ensures that the continued privacy of Canadians remains fundamental in the overall transaction and in the collection, use and disclosure of information.

Mr. Tony Van Bynen: You mentioned earlier that by stipulating these—

The Chair: Thank you, Mr. Van Bynen. I'm sorry, but we'll get back to you when we come back to Bill C-27. We've reached the end of our meeting.

I appreciate, members, your co-operation during this meeting.

[*Translation*]

Thank you, everyone.

I want to thank the witnesses.

Have a good day.

The meeting is adjourned.