HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

44th PARLIAMENT, 1st SESSION

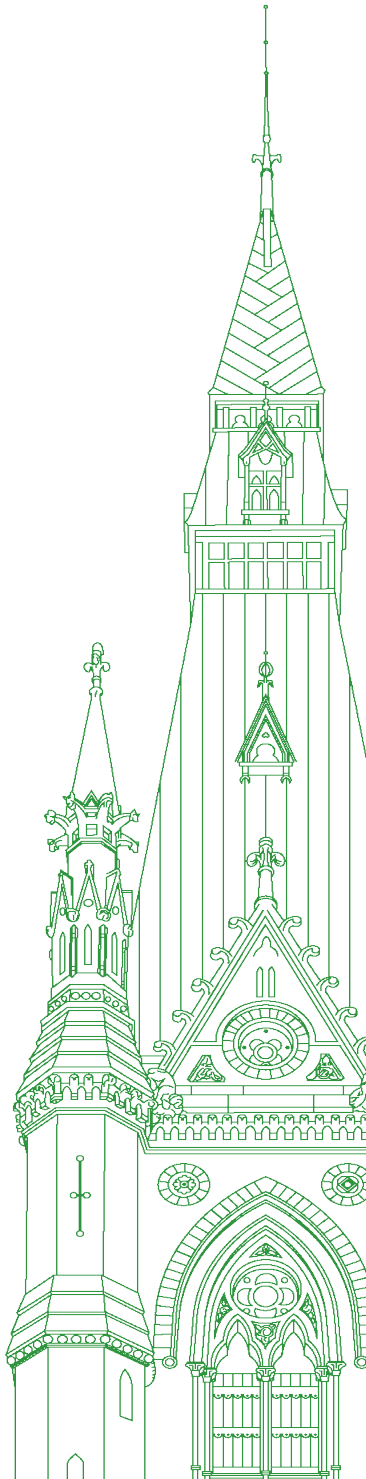
Standing Committee on Industry and Technology

EVIDENCE

NUMBER 100

PUBLIC PART ONLY - PARTIE PUBLIQUE SEULEMENT

Thursday, November 30, 2023



Chair: Mr. Joël Lightbound

Standing Committee on Industry and Technology

Thursday, November 30, 2023

● (1555)

[*Translation*]

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

Welcome to meeting No. 100 of the House of Commons Standing Committee on Industry and Technology. This is a bit of a special occasion.

I would also like to note that this is the birthday of our analyst, Alexandra Savoie. We wish her a happy birthday and thank her for her help with this important study.

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

I would like to welcome the witnesses and also apologize for this meeting starting late.

Our witnesses are Sébastien Gambs, Canada research chair in the privacy-preserving and ethical analysis of big data, who is participating by videoconference from the Université du Québec à Montréal, and Philippe Letarte, head of policy and public affairs at Flinks.

From Option consommateurs, we have lawyers Sara Eve Levac and Alexandre Plourde. And last, we have Sehl Mellouli, deputy vice-rector of education and lifelong learning at Université Laval, who is joining us by videoconference.

Welcome, everyone.

With that, I will not take up any more time. We will start with the opening remarks without further delay.

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

Mr. Sébastien Gambs (Canada Research Chair, Privacy-Preserving and Ethical Analysis of Big Data, Université du Québec à Montréal, As an Individual): Hello and thank you for inviting me and offering me the opportunity to address you.

I am going to give my presentation in French, but then I will be able to answer questions in English or French. In these five minutes, I am going to try to focus on the concepts of privacy, explainability and fairness in artificial intelligence.

First, there is an important element that does not seem to be addressed in the bill. When you are training a learning model, essentially, it will summarize the personal data that was used for training it. An assessment of the privacy-related factors will therefore have to be done, taking into account state of the art attacks. In my research community, for example, we try to show that using a learning model, or a "black box", like a neural network, training data can be reconstructed.

In addition, a challenge that we will have in the future, and that we have now, is that most learning models that people develop are improved using pre-trained models that were themselves trained using personal data that we do not necessarily know the origin of. I would therefore say that there are going to be very considerable challenges in this regard, in particular in the case of high-impact artificial intelligence systems.

We can also see that there are going to be difficulties regarding the creators and users of the models. For example, in the bill, section 39 of the Artificial Intelligence and Data Act says that people are responsible for the use of a learning model, but when we talk about foundation models, which are the basis of tools like ChatGPT, those models can be used for a lot of things. It is therefore difficult for the creator of a model to predict all the beneficial or harmful uses that could be made of it, and so, in practice, we have to distinguish between the person who created the model and the use made of it in a particular case.

Regarding explainability, which is the second important subject, apart from providing an explanation to someone about the reason for a prediction, they also have to be given a clear explanation of what data was collected, the final result, and the impact on the individuals. It is particularly necessary to be transparent in these regards and to provide a comprehensible explanation in the case of high-impact artificial intelligence systems so the person has remedies. Without a good explanation, essentially, they cannot question the decision made by the algorithm, because they do not understand it. In the case of high-impact systems that affect people, they should also have the ability to contact a human being, somewhere in the process, who has a solution that allows for the decision to be reviewed. This is a concept that is missing in the bill.

Overall, therefore, an impact analysis has to be done that takes into account not only privacy-related factors but also these ethical issues. I have not mentioned fairness, but that is also an important point. Apart from the law, another challenge we are going to encounter will be to adopt standards based on the fields of application, in order to define the correct fairness indicator and incorporate it into artificial intelligence systems, and the right form of explanation to offer. It will not be the same in the medical field as it is in banking, for example. The protection mechanisms to put in place in each context will have to be defined.

I would like to conclude my presentation by talking about the risk associated with fairwashing, an issue I have done some work on. Essentially, it requires concrete standards that define the fairness indicator to be used in a particular context, because there are many different definitions of fairness. Debates have already arisen between companies that built artificial intelligence systems and researchers regarding the fact that a system was discriminatory. The company said the right indicator had not been used. Without precise standards put in place by the stakeholders, therefore, companies could cheat and say that their model does not discriminate, when they have chosen a fairness indicator that works to their advantage. It is also very easy to come up with explanations that seem realistic but in no way reflect everything the "black box" does.

I would therefore say that the fairwashing issue could become apparent when the bill is put into effect. We have to think about ways of avoiding this and adopt concrete standards that will not necessarily be in the legislation, but will be defined afterward, to avoid the legal uncertainty surrounding fairness indicators and forms of explanation relating to privacy issues.

Finally, if I have 30 seconds left, I would first like to address one last point regarding privacy. The difference between the definition of anonymized data and the definition of de-identified data is always difficult for me, because, as a privacy researcher, I know there is no perfect method of anonymizing data.

The bill refers to anonymized data, an irreversible process, and de-identified data, a process that could be reversed someday. In fact, I think there really is no perfect method. Therefore, even when we are told that data is anonymized, in general, there are always risks that it will be possible to identify the person again by cross-referencing with other data or other systems. The difference between the definitions of these two terms could be clarified, or in any event should be clarified by providing additional explanations.

I hope I have not gone too far over my speaking time.

● (1600)

The Chair: It's fine. I am pretty liberal with time, but thank you for being mindful of it. We were close to the limit.

Mr. Letarte, from Flinks, you now have the floor for five minutes.

Mr. Philippe Letarte (Head of Policy and Public Affairs, Flinks): Thank you, Mr. Chair.

I want to thank the members of the committee for having me here today.

My name is Philippe Letarte and I am head of policy and public affairs at Flinks Technology Inc.

Flinks is a technology company founded in Montreal whose mission is to enable consumers to control their finances and to create a customer-centred banking environment. That banking environment, which is also called an open banking system, is based on consumers' ability to control and direct the use of their financial data so they are able to receive the best financial services and products available to them.

To facilitate the discussion period and avoid any potential confusion relating to the technical terms, I am going to continue the rest of my address in English.

[*English*]

Flinks is pleased to see that the notion of control, or “consent” in the context of privacy legislation, is apparent throughout the CPPA, which, once enacted, will clearly constitute the cornerstone of all activities organizations engage in that involve the processing of personal information. This is a much-needed overhaul of the CPPA’s predecessor. It will introduce a more consumer-protectionist approach to processing activities, while also moving Canada’s privacy regime closer to what has been established across other OECD countries. Flinks is pleased to see that consent will now form the basis for all personal information processing activities.

As previously mentioned, one of Flinks' raisons d'être is to give consumers control over their personal and financial information, and more specifically to direct how such information is used and by whom. Inherently, this involves many participants in the ecosystem in which Flinks currently operates.

We do, however, remain concerned about the following wording set forth in proposed section 72 of the CPPA: “if both organizations are subject to a data mobility framework.” This proposed language raises questions related to how an organization takes part in this framework, whether there will be multiple frameworks for different types of organizations, what limits are in place if a given organization is not part of said framework, and what the requirements will be to remain compliant with such a framework.

This language is also incompatible with the proposed language in last week's fall economic statement and the policy statement on consumer-driven banking, which states that the federal “government will mandate participation for federally-regulated” entities.

It is now an indisputable fact that jurisdictions with successful open banking regimes have not only forced the participation of an overwhelming majority of their financial institutions and third parties in the framework but have also, because of strong and clear regulations, given confidence to consumers that adequate protections were put in place.

With the current wording, there's a risk of inadequacy in CPPA and upcoming future consumer-driven banking regulations, in terms of which entities and datasets are covered by which framework, leaving Canadian consumers confused, and depriving them of the benefits of customer-driven finance. We therefore recommend changing the wording of proposed section 72 to make the participation in the data portability framework mandatory for organizations in the financial sector—not "if", but "when"—and to avoid any potential loopholes or flaws among different regulations dealing with data portability rights.

We also have concerns about the concept of the "legitimate interest" exception to consent in proposed subsection 18(3) and proposed subsection 18(4) of the CPPA. The inclusion of this exception appears to lend itself to abuse in the absence of any further guidance or clarification, as no definitions are provided for "legitimate interest" or "adverse effect". This creates the possibility of a scenario in which organizations are left to conduct their own assessment as to what the weights of a legitimate interest and adverse effect are, without any further information to rely upon in doing so. This is problematic, as an organization may, for example, seek to use the "legitimate interest" exception as a way of curtailing any limits the CPPA places on consent or on secondary uses of personal information. This type of interpretation or application of a legitimate interest by a participant in an open banking environment would completely erode any trust in open banking in Canada.

In light of this, please allow us to respectfully recommend clarifying this provision by establishing clearer definitions or providing assessment criteria for what a "legitimate interest" and an "adverse effect" are. In the same vein, we respectfully ask the committee to also clarify the types of scenarios or criteria for determining what is "clearly in the interests" of an individual, as mentioned in proposed subsection 29(1) of the CPPA.

In conclusion, I would like to reiterate the urgent need for Canadians to benefit from a true customer-driven banking system. Since the advent of the digital economy, not a great number of public policies have proven to be as beneficial as open banking. It helps drive competition and innovation in a very concentrated and archaic sector. It empowers consumers to make better-informed financial decisions while giving them control over their own data. It enhances the financial inclusion of the most vulnerable. It reduces drastically the cost of operation for small business owners and it stimulates entrepreneurship and foreign investment, and so on.

● (1605)

The measures proposed in the fall economic statement, doubled with the provisions and protections established by the CPPA, represent a unique opportunity to provide Canadians with financial freedom and adequate privacy protections while bridging the competition gap with trading partners and other modern economies.

I am happy to answer any questions the committee may have to the best of my capabilities.

[*Translation*]

I will answer equally well in French and English.

The Chair: Thank you, Mr. Letarte.

I believe Mr. Vis would like to ask you a question about the section you mentioned.

[*English*]

Mr. Brad Vis (Mission—Matsqui—Fraser Canyon, CPC): Mr. Letarte, did you specify paragraph 21 or 29 near the end of your remarks?

Mr. Philippe Letarte: That would be proposed subsection 29(1) in clause 2.

Mr. Brad Vis: It's proposed subsection 29(1). Thank you.

[*Translation*]

The Chair: Thank you.

I will now give the floor to the representatives of Option consommateurs. Ms. Levac or Mr. Plourde, you have the floor.

Mr. Alexandre Plourde (Lawyer and Analyst, Option consommateurs): Hello, Mr. Chair and members of the committee.

Thank you for offering us the opportunity to present our comments.

My name is Alexandre Plourde. I am a lawyer with Option consommateurs. With me is my colleague Sara Eve Levac, who is also a lawyer with Option consommateurs.

Option consommateurs is a non-profit association whose mission is to help consumers and defend their rights. As a consumers' association, we are in regular contact with people who are having privacy-related problems. In recent years, we have often become involved in privacy issues, for example by publishing research reports and taking part in consultations on proposed legislation. We have also initiated large-scale class actions, including under the federal Privacy Act.

As you can read in the brief we have submitted to the committee, Bill C-27 contains a number of flaws, in our opinion, particularly regarding the exceptions to consent, the absence of a right to be forgotten, the limitations on the right of portability, and management of individuals' data after their death.

Since our time is limited, we will first address two aspects of Bill C-27 that are of particular concern to us.

First, I am going to talk about Bill C-27's lack of deterrent effect and the obstacles this may create for civil actions by consumers. Second, I am going to talk about the flaws in relation to children's privacy.

Our first concern relates to Bill C-27's lack of deterrent effect. We believe that the bill contains flaws that could make enforcing it problematic. First, although the bill contains high administrative monetary penalties, only certain violations of the act can result in such penalties being imposed.

Second, the Privacy Commissioner will not have the power to impose penalties directly; they will be able to do so only by recommending to the new personal information and data protection tribunal that penalties be imposed. That additional step suggests, at least, that there will be significant delays in applying the penalties imposed on businesses that commit offences.

In addition, the deterrent effect of legislation is also based on the public's ability to rely on it in the civil courts. However, we believe that the new private right of action provided in proposed section 107 in the bill seriously threatens consumers' ability to apply to the courts to exercise their rights. The problem arises from the fact that the new private right of action allows a company to be sued only if prerequisites are met, requiring, in particular, that the situation have first been dealt with by the Commissioner.

In our opinion, it is entirely possible that the big companies targeted by class actions will rely on these very stringent conditions in order to defeat the legal actions brought against them. There will then be interminable proceedings in the courts to determine the scope of the federal private right of action, given the provinces' constitutional jurisdiction over civil law.

We therefore invite the government to clarify that section 107 is in addition to the other civil remedies provided in provincial law, to ensure that it does not obstruct civil actions instituted under Quebec law.

I will now give my colleague, Ms. Levac, the floor.

Ms. Sara Eve Levac (Lawyer, Option consommateurs): Our second concern relates to flaws in relation to children's privacy. Those flaws are still present despite the amendments announced at the start of the consultations.

Although Bill C-27 recognizes the sensitive nature of minors' personal information, we believe it does not go far enough to really protect children's privacy. We propose that the protection provided by this bill be strengthened by incorporating the best practices recognized in international law.

First, the bill has to offer stronger protection for children in the digital universe, by protecting them from commercial exploitation of their personal information. The web applications that children use may collect countless pieces of data about them. That data may then be used for profiling or targeting the children for commercial purposes. There is nothing in Bill C-27 that prohibits those practices.

Second, the act should provide that decisions concerning a child's personal information must be made in the child's best interests. The concept of the best interests of the child provides for a more comprehensive vision of privacy than mere recognition of the sensitive nature of the child's personal information. For example, it allows for an assessment of whether the use of the child's personal information by a business promotes his or her overall development and whether the child's rights are being exercised for his or her benefit.

For example, it might not be in the child's interest to give the child's parents or guardians access to his or her personal information where the child is being abused by them. An analysis based solely on the sensitive nature of the personal information would not limit access of that kind.

We will be pleased to answer your questions.

● (1610)

The Chair: Thank you.

We will now give the floor to Mr. Mellouli, who is joining us by videoconference.

Mr. Sehl Mellouli (Deputy Vice-Rector, Education and Lifelong Learning, Université Laval): Thank you for the invitation and for this opportunity to speak about the artificial intelligence bill and its application to data.

I am not going to reiterate some of the things that Mr. Gambs discussed earlier. However, I would like to come back to certain things in the bill that are not entirely clear, in my opinion, or that should be clarified, particularly when we are talking about biased output. This is one of the things that caught my attention: what is a biased output and how is a biased output arrived at?

Artificial intelligence will never give 100% true output. It is always based on learning, and that learning is what determines that it gives a recommendation or decision, or that it generates new information, new data.

If a person is the subject of biased output, is that the responsibility of the business or organization that created the bias? Is a bias normal? A machine learning system might have a certain degree of success, 90% or 97%, for example. Artificial intelligence will never be 100% true, today. What caught my attention is really the definition of biased output.

I want to draw attention to the learning and the data. Learning takes place using data, but the business has the complete ability to fragment the data among various organizational structures. A piece of data, of information, can even be transformed. The bill raises the fact that there would have to be information about how data is managed and how it is anonymized.

There is also anonymous or de-identified data, as was mentioned. But how can we make sure that the business has not fragmented that data in such a way that it could retrace it? That information cannot be fund in an audit. This is a very important factor to consider in terms of enforceability. I can present you with an entire manual that shows that I have properly anonymized my data and how I manage it, but you cannot be certain that what I used for the learning was that anonymized data. Even if we can go back to find out a bit about the data that was used, as Mr. Gambs said, that is always going to be a difficult and relatively complex job to do.

The last point I would like to address is when we talk about a high-impact system, as you define it. We can say that it is the loss of confidentiality, integrity or availability of data that may have serious or catastrophic consequences for certain individuals or certain entities. If the business defines its system as having a 97% success rate, that means it will always have a 3% failure rate.

So does the case you are looking at fall into that 3%? How can we determine that we are in one of those situations, where a prejudice or bias against a very specific person is created, in spite of the fact that the learning was done correctly?

There are therefore a number of challenges relating to the data that you use: how do you make sure that it is anonymous, that it has not been fragmented or modified? The business will have the complete ability to retrace the data, but an auditor who wanted to do the same thing would find the job very complicated and very complex.

Even if things are done very properly, what is a bias and what is a biased output? How do we make sure that biased output, which does not work and which harms an individual, does not fall within the 3% failure rate in the learning?

Thank you. I am available to answer your questions, in English and French.

● (1615)

The Chair: Thank you, Mr. Mellouli.

To open the discussion, I am going to give Mr. Généreux the floor for six minutes.

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

Thanks to all the witnesses for being here today.

Mr. Mellouli, I am going to start with you; I think I was the one who invited you, through your president. Are you from the Université de Montréal or Université Laval?

Mr. Sehl Mellouli: I am from Université Laval.

Mr. Bernard Généreux: As luck would have it, I went to visit Université Laval in September. I realized when I was there that that university is in a good position to do research on artificial intelligence.

I imagine you are a researcher yourself. In any event, you seem to be very familiar with the subject.

In your remarks just now, you talked about biased output, accountability on the part of businesses, and fragmentation of data. When you talk about learning, in the language of artificial intelligence, what distinction do you make between learning and anonymization? I want to be sure I understand.

Mr. Sehl Mellouli: I will be happy to answer your question. I want to make sure I understood it.

Let's talk about anonymous data. Assume that for the machine's learning, I do not use a person's name, or their race or origin, or social insurance number...

Mr. Bernard Généreux: Forgive me for interrupting, but could you give me the definition of learning?

Mr. Sehl Mellouli: Learning is when we give a machine a certain amount of data. The learning may be supervised or not, and I am going to limit my remarks to those two types of learning.

In the case of supervised learning, the machine is given a body of data that will be identified. For example, you say that Sehl Mellouli is a professor. You can add that he belongs to an ethnic minority or his behaviour is excellent, average or bad, for example. That is how you do it so that the system learns from the data you have identified.

As a result, the system can use personal data about Sehl Mellouli to carry out learning by identifying the data that say what kind of person he is, without anonymizing that data. From that personal data, the system can learn.

If the data is anonymous, so much the better. If it is not anonymous, the system will learn from data that is not anonymous and will be able to profile Sehl Mellouli based on a context it chooses, such as his origin, his accent, or what kind of person he is.

Mr. Bernard Généreux: That explains the possibility of a 3% error rate. You refer to that 3% risk. You talked about potentially biased output. Is that right?

Mr. Sehl Mellouli: That's right.

I always tell my students that if their system gives them results that are 100% correct, there is a problem. This is a computer program that is learning. When you learn from hundreds of thousands of pieces of data, you cannot be certain that all the data being used for learning is right. Systems always have degrees of success, which are used to evaluate their capacity.

Take ChatGPT, for example. It may give you the right answer to a question today, but it may also give you the wrong answer sometimes.

● (1620)

Mr. Bernard Généreux: Yes, we have seen that several times in the past.

Are the 97% and 3% degrees of success and error therefore standard percentages in the industry, or do they represent a target you aim for yourself?

Mr. Sehl Mellouli: It depends. They are not industry criteria and Mr. Gambs can correct me if I am wrong.

The success rate is used to evaluate the systems. If you are building a new system, you sometimes compare its success rate to the one for other systems or other algorithms. You are trying to create the best learning system possible. Sometimes you may find one that gives a 90% success rate, compared to others for which it is 80%.

Some researchers are working on improving the capacities of these learning systems in order to expand them or increase the success rate of predictions in terms of the output obtained.

Mr. Bernard Généreux: The other thing you talked about is high-impact systems, whose output resulting from the system's success rate and the collection of the data used may have serious repercussions. Do you see this as a risk? With respect to the proposed legislation or the description of it, what changes would you propose?

Mr. Sehl Mellouli: I can't propose something that could be changed. I'm saying that you should really compare the system's ability to behave well with the risk that it may make mistakes. With the artificial intelligence systems available today, I think you have to allow for a margin of error because, even though the systems have a very high degree of reliability, they aren't 100% reliable.

That's why I mentioned the loss of confidentiality and data integrity or availability that may have serious impacts on certain persons. How many of the total number of persons concerned by the system have been affected? If 80% of those people are seriously affected, we really have a high-impact system, and action has to be taken. On the other hand, if barely 1% of 100,000 individuals are affected, that percentage may fall within the learning rate, which allows the system to make mistakes in 1% of cases.

Mr. Bernard Généreux: So even artificial intelligence isn't perfect.

Mr. Sehl Mellouli: No.

Mr. Bernard Généreux: Thank you very much.

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

Ms. Lapointe, the floor is yours.

Ms. Viviane Lapointe (Sudbury, Lib.): Thank you, Mr. Chair.

Mr. Letarte, do you think that the legislation includes appropriate measures to enable businesses to comply with it?

Mr. Philippe Letarte: I think it's already a good start for businesses, and that, incidentally, is why I'm here.

I know that the sharing of bank information isn't necessarily the main subject matter of Bill C-27, but I think the bill lays the foundation for the legislative framework promised in the fall economic update. It's currently the closest thing to something that enables data sharing and portability.

I also think you should establish stricter terms and conditions and insert them in a regulatory division following from Bill C-27 or in a future bill directly concerning an open banking system.

Ms. Viviane Lapointe: Thank you.

We understand that, if the legislation on privacy protection and artificial intelligence isn't harmonized globally, the efficacy of those statutes and rules will be compromised. What you think of the way the various authorities can work together to implement standards?

Mr. Philippe Letarte: Are you asking that question with respect to artificial intelligence?

Ms. Viviane Lapointe: I'm interested in privacy protection and artificial intelligence.

Mr. Philippe Letarte: It's actually important to understand that the consumer banking system has a virtually global presence. Canada is one of the last countries where there is no right to data portability. Many countries that are very close to us in the Commonwealth, such as Great Britain and Australia, as well as the entire European Union and certain Asian countries, have that kind of system, and we can already see how easy interoperability is among those countries.

I think it's time for Canada to step into the modern world and grant Canadians the right to portability. As for interoperability, I'd say it's not very complex. The rules are quite similar.

I'll refrain from commenting on artificial intelligence because I'm not an expert in that field. It's an extremely complex subject. I think everyone's trying to understand this, including the president of OpenAI, who was fired and then rehired. So I'll refrain from commenting on the subject in the context of a piece of general legislation.

● (1625)

Ms. Viviane Lapointe: Some witnesses noted that the pop-up windows requiring consent on many sites and applications are of no interest because people don't read the text and only click on "Yes" so they can continue.

What do you think of informed consent, the right to privacy and corporate organizational responsibility? Should the organization be responsible for informed consent?

Mr. Philippe Letarte: Absolutely. That's why we're very pleased that Bill C-27 was introduced. Our business currently operates in a system that lies in a kind of grey area and that hasn't been extensively legislated. We've been asking the federal government to intervene on behalf of consumers for a very long time now.

You mention pop-up windows. From our viewpoint, it's much more precise than that and more highly regulated. If you have an online app to do your accounting or manage your retirement or investments, you will have to give consent. We want that consent to be adequately protected and renewed as well.

Although our case is a bit different from anything involving cookie files and pop-up windows, we want regulations to be added that give consumers the power to consent to their data being shared and that guarantee them adequate protection. Let's be honest: there are two taboos in society, and they are our finances and our personal information. Here we're combining the two.

So, to sum up, it's important to have adequate protection, and, as far as we're concerned, just as important that consent have to be given. For all the systems and authorities I mentioned earlier, businesses should be responsible for getting consent.

We're very pleased with the content of the bill because it will create a legislative framework that's safe and therefore more effective for consumers. That will also enable our business to grow in an environment that's secure and stable.

Ms. Viviane Lapointe: Mr. Plourde or Ms. Levac, I'd like to ask you the same question.

Mr. Alexandre Plourde: Consent is indeed one of the methods for protecting consumers. It's the method that has mainly been used in this bill. Something else could have been chosen, and other protection standards could have been added, but what we still have here is legislation that hinges on consent. Consent can be a method that operates to protect consumers in the digital environment and enables them to control their information, provided that consent is effective and can genuinely be useful to consumers.

Bill C-27 poses a problem with regard to related exceptions to the requirement of consent. We feel that those exceptions are too broad. The exception that concerns us most is the one provided under clause 18, for the purpose of business activities and legitimate interest. This is an exception that we consider too broad. We find it hard to understand how it can be consistent with the implicit consent that already exists. We therefore suggest deleting clause 18, which would allow businesses too much leeway to use consumers' information without their consent.

You also mentioned pop-up windows at the start of your question. It seems to me you're referring to the concept of consent fatigue, which occurs as a result of being constantly asked to give your consent. People are bombarded with demands and requests for consent, and we're aware of this concern about consent fatigue.

We think that businesses should show some creativity. The bill should also offer effective solutions enabling consumers to express a blanket refusal to be tracked online. When we go onto various websites, mobile apps and tech company platforms, our privacy and data are permanently captured for those businesses to use for commercial and other purposes. The current method is to have us consent singly to each business when pop-up windows appear.

The solution we suggest in our brief is that we instead create mechanisms enabling consumers to state a blanket refusal to allow their browsing data or other personal information to be transmitted to any companies with which they do business. This is what we call the "do not track" mechanism, which is already available in web browsers but isn't recognized by businesses. We propose that businesses be required to recognize this kind of signal or parameter that, with one click, enables people to send a blanket refusal to provide their personal information. This would put an end to the consent fatigue we all dislike.

● (1630)

Ms. Viviane Lapointe: Thank you.

The Chair: Thank you, Ms. Lapointe.

I rarely do this, but, with your permission, I would like to ask the witness a question.

Mr. Plourde, I find what you just said very interesting. From what I understand, some online browsers like DuckDuckGo allow blanket refusals to provide personal information. Do you have a specific proposal to amend a clause of the bill?

Mr. Alexandre Plourde: That's a very good question. It could be included in the clause on consent. I can't remember the exact clause, but one of them provides that consent must be implied. You could word it so that consumers may indicate a general refusal to share their information, which could target certain types of information such as a person's browsing data or usage data from a person's digital devices.

Consumers could indicate their refusal through an interface or some technology, and businesses would have to honour that refusal. It might not be that technically difficult to integrate because web browsers already have these kinds of parameters. It would simply be a matter of compelling businesses to honour consumers' wishes.

The Chair: If by chance you have a proposal to submit to us, please feel free to do so. We still have time in our study. It would be a pleasure for us to consider it.

I'm quite concerned about this consent fatigue as well. Sometimes it seems to me that we attach a lot of importance to consent. I understand why, but it should be of limited value, as Ms. Lapointe mentioned, considering that no one reads conditions. You often click on "Accept" just to speed up the process.

Mr. Letarte, I'd like to have one final clarification: what specifically does data portability mean for consumers of financial products?

Mr. Philippe Letarte: Technically speaking, no one in Canada currently owns his or her financial data. You deal with the bank, and you have an online account and probably a checking account and a mortgage. All that generates data, including basic information such as your address. Currently, if someone wants to purchase another financial product offered by another bank, that individual's bank may refuse to pass on the customer's financial information because the customer doesn't own it.

I'm going to give you a brief history of the right to data portability. It wasn't invented by the private sector or technology companies. It's actually the result of a legislative proposal made in the United Kingdom by Competition & Markets Authority following the 2009 financial crisis. CMA claimed that the banks hadn't championed the rights of consumers and that there was an excessive concentration in that sector.

In its report, entitled "Making banks work harder for you", CMA stated that the right to portability was the solution. In other words, consumers should be granted the right to take their financial data and do business with the institution of their choice, which would enable them, for example, to compare mortgage rates, various investments and different percentages and interest rates in effect for checking and other accounts.

The policy snowballed. As I said, most OECD countries and, I believe, the 70 largest economies now acknowledge the right to data portability. Australia has been a little more ambitious: it uses data portability in other sectors, such as telecommunications and energy.

Does that answer your question?

The Chair: Yes, thank you very much.

We now return to our regularly scheduled programming.

Go ahead, Mr. Lemire.

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

Mr. Gambs, with your permission, I'd like to benefit from your expertise.

Yesterday, Radio-Canada revealed that government departments and agencies were using spying equipment initially associated with the intelligence community to recover and analyze data, including encrypted and password-protected information. Furthermore, the use of those surveillance tools had apparently not been subject to a privacy risk assessment, despite a federal directive requiring it.

In the circumstances, considering that the public sector is included in Bill C-27, what are the main concerns regarding the use of these types of surveillance tools by government entities and, more particularly, the failure to conduct privacy risk assessments?

● (1635)

Mr. Sébastien Gambs: I'll be brief. The risks are enormous, and the reason for using those tools seems debatable to me.

For the moment, based on the information that has come out, the reason why those tools were used isn't very clear. Furthermore, I believe that a government should be irreproachable, since the bill requires businesses to conduct privacy impact analyses and to show that their practices are exemplary.

I don't need to provide any details, but those tools are used to monitor activists and journalists. People have gone to prison or died as a result of those kinds of tools, which are also used in certain totalitarian countries and countries that monitor political opponents. I think those revelations should be subject to an in-depth analysis and investigation.

Mr. Sébastien Lemire: Is it necessary to extend the provisions of this bill to the private sector to guarantee complete protection for the data of Quebeckers and Canadians? At the same time, how could Bill C-27 be adapted or reinforced to ensure adequate regulation of the use of these kinds of tools in the public sector?

Mr. Sébastien Gambs: I think you should add a clause providing that those surveillance tools definitely not be used to collect data for which consent has been obtained from the persons concerned. That clause should focus specifically on how those surveillance tools should be controlled and ensure that the use of those kinds of tools is subject to significant guardrails.

I imagine there could be strict national-security exceptions. However, from what I understand about the revelations, many departments use those tools in situations that have nothing to do with national security. Consequently, I think it's necessary that you add a specific clause framing the options for using those tools and impose guardrails, in addition to significant judicial control.

Mr. Sébastien Lemire: Given the emergence of quantum technology in the next few years and the fact that it will be covered by the bill, I believe that guarantees and surveillance mechanisms are necessary. What guarantees and surveillance mechanisms could effectively protect the information and data of Quebeckers and Canadians?

Mr. Sébastien Gambs: The quantum field will have an impact on many aspects of communications security, not just on data monitoring tools.

I think that the security standards that are being developed by the National Institute of Standards and Technology in the United States and that will apply to the Internet already reveal a willingness to provide security tools that will help resist quantum attacks.

I don't know whether Bill C-27 mentions anything regarding post-quantum resistance. Apart from data-monitoring tools, that may concern personal data or data security in general.

Mr. Sébastien Lemire: Ms. Levac or Mr. Plourde, Bill C-27, which will replace the Personal Information Protection and Electronic Documents Act, will give consumers a new right to explanations for the use of automated decision systems to make predictions, provide recommendations and make important decisions concerning them, even when the data used have been depersonalized.

However, unlike Quebec's Bill 25, Bill C-27 makes no provision enabling anyone to oppose the use of an automated decision system or to review a decision made by such a system. What do you think are the potential repercussions for consumers of the absence of any such provisions from the bill?

Ms. Sara Eve Levac: Currently, Bill C-27 would allow someone to obtain on request an explanations of automated decisions. We propose that this should go further, somewhat as you explained with the Quebec example.

First, it may be difficult for consumers to determine whether a decision concerning them was an automated decision. For example, when credit card applications are denied, no explanation is provided to the applicants that would let them know the decision concerning them may have been automated. Consequently, we would recommend that Bill C-27 provide for an obligation to inform consumers that the decision concerning them was an automated decision.

Then we could request that Bill C-27 provide that explanations be provided regarding that decision. An additional step would be to provide as well that a human being may review a decision made by an automated tool, somewhat as is possible in Quebec, so that person can make observations.

There have been media reports of cases in which people were denied credit because the information considered in making the decision included errors. The possibility that such decisions can be reviewed could therefore help avoid situations in which consumers are denied contracts or loans because the decisions concerning them were based on false information.

● (1640)

Mr. Sébastien Lemire: So I understand that you are in favour of including provisions similar to those in Quebec's Bill 25 in Bill C-27 to strengthen it.

Who could be called upon to challenge an automated decision?

Ms. Sara Eve Levac: As is the case with Bill 25, in Quebec, we propose that consumers who have been the subject of a decision made by an automated system be able to go to the company that used that system in order to make their case and to ask that the decision concerning them be reviewed by a human from that company.

Mr. Sébastien Lemire: Thank you.

The Chair: Thank you, Mr. Lemire.

Mr. Masse, you have the floor.

[*English*]

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

Thanks to our guests for being here, and thanks to those online.

I'll start with those online and then turn to our guests here.

We have two models with regard to the Privacy Commissioner position: either empowering the Privacy Commissioner and going with that model, or going to a tribunal, which will dilute the Privacy Commissioner's capabilities. I'm just curious. You almost have to pick one at this point, because the tribunal will be new.

Maybe I'll start with our online guests—I can't see their names right now, Mr. Chair, so maybe you can pick—and then I'll go across the table here to get your opinions as to what you would do if you were in our position.

We'll start with Mr. Gambs and then go from there.

If you had to pick one of those models, which one would it be?

Mr. Sébastien Gambs: I think it will be to empower the Privacy Commissioner, especially, since you also need to add expertise on explainability and also on fairness, so I would basically try to leverage expertise on privacy but also supplement that with expertise on other ethical issues. I think that being able to conduct an analysis on all these topics seems to be the best idea.

Mr. Brian Masse: Go ahead, Mr. Mellouli.

[*Translation*]

Mr. Sehl Mellouli: Allow me to answer you in French, in the same vein as Mr. Gambs.

It is important to have the ability to increase control over the use of personal data in artificial intelligence systems. In my opinion, instead of looking at AI learning systems—and there are a number of them—the only process that would be important to examine further is the data we are going to learn about. That's the challenge.

How can we help the commissioner ensure that the right data was used to learn? That's my only concern. I say this and I repeat it, as these systems are “black boxes”, and it is not easy when it comes to many, if not hundreds of thousands, of pieces of learning data, to recover the data that was used for learning.

What checks and balances can be put in place? In my opinion, this aspect deserves more thought, but unfortunately I really don't have any solutions to propose today.

[*English*]

Mr. Brian Masse: Thank you.

We'll go to our guests here.

[*Translation*]

Mr. Alexandre Plourde: If I understand your question correctly, you're asking about the model of the personal information and data protection tribunal proposed in the bill. Is that correct?

[*English*]

Mr. Brian Masse: Well, yes, does the Privacy Commissioner have a tribunal that's going to decide the penalties and so forth or is it empowering the Privacy Commissioner to have those capabilities? If we create the tribunal, it creates its own entity of punishment and correction of behaviour and so forth, versus having that come from the hands of the Privacy Commissioner.

● (1645)

[*Translation*]

Mr. Alexandre Plourde: That is one of the problems that Option consommateurs raised in its brief. There are some good aspects to Bill C-27, since the Office of the Privacy Commissioner of Canada is given the power to issue orders, and the bill provides for administrative monetary penalties of up to $10 million or 3% of sales. That's meaningful.

However, this punitive system does have flaws. The office of the commissioner will only have the power to recommend these administrative monetary penalties, which only the specialized tribunal can then impose. This process seems to us too long and unnecessary. Furthermore, these administrative monetary penalties do not cover all breaches of the act. We believe that any breach of the act should be subject to an administrative monetary penalty, imposed directly by the office of the commissioner.

We see no reason to delay the imposing of such a penalty by referring the matter to a court. If the office of the commissioner chooses to impose an administrative monetary penalty, it is because it has made numerous representations regarding that company, it has warned it several times and the decision is carefully considered. So I don't see why the process would be slowed down.

In Quebec, the Commission d'accès à l'information du Québec can directly impose administrative monetary penalties. Recently, a new bill was passed in Quebec that enables the Office de la protection du consommateur to impose administrative monetary penalties directly, as well. We do not see why the federal government could not do what's being done in Quebec.

[*English*]

Mr. Brian Masse: Thank you.

Mr. Letarte, would you like to comment?

Mr. Philippe Letarte: We don't have any particular opinion on that front.

That being said, in the fall economic statement, it was said that in order to enforce customer-driven banking finance, they need to have some form of government entity. Is it the Office of the Privacy Commissioner? If yes, it should add additional resources or manpower to do so, but we're not for or against any specific tribunal versus giving this power to the Privacy Commissioner.

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

[*Translation*]

The Chair: Thank you, Mr. Masse.

[*English*]

Mr. Williams, the floor is yours.

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

Thank you to all our witnesses.

Mr. Letarte, it's nice to have you here today. I introduced a bill about a month ago in Parliament to make sure that consumer-led banking—open banking—gets going. Actually, I'm going to have a bet with my colleague from Abitibi-Témiscamingue—about $50—on whether we'll get third reading of Bill C-27 first or open banking first. I'm not sure. I think I can win some money off him.

Voices: Oh, oh!

Mr. Ryan Williams: The premise of this is that it seems these are actually in the right stride, parallel to each other. Bill C-27 deals with data. For those listening at home, the whole premise around consumer-led banking is really to make it mandatory that the banks have to share your personal data with other entities who can bank you, which allows.... In the U.K., where we saw it with 4,000 companies, U.K. residents are saving 12 billion pounds a year and businesses eight billion pounds a year. It's really great.

My first question for you as we look at the key to unlocking consumer-led banking is this: Can consumer-led banking, open banking, exist without this legislation right now?

Mr. Philippe Letarte: I will say from the get-go yes, but I think Bill C-27 is a really good first step into those regulations. It really lays the foundation upon which we can build and it levels the playing field about modernization and privacy in this country, which is greatly overdue.

In terms of my own interests, I hope we're going to get open banking sooner rather than later. I really believe it is kind of an emergency to have open banking at this point in time, for several reasons.

First, we know that the cost of living in Canada is problematic. We know that we need to give more resources to Canadians. We also know that we are losing competitiveness on international ground, so whatever gets it done the fastest is good, but Bill C-27 is a good foundation upon which we can build.

Mr. Ryan Williams: Okay. I'm going to focus on how this industry can thrive with this legislation.

You had three amendments, and I want to focus on those. I'd like you, on each one, to just elaborate a little bit more about exactly what we need. If you have wording that you'd like to see in an amendment, you can submit it to the clerk—which is probably the best way—so then we will have that.

Let's start with legitimate interests.

You mentioned proposed subsections 18(3) and 18(4). Just elaborate a little bit more on those, and if you want to go through all three of them, then it's proposed section 72 and then proposed subsection 29(1). Just walk us through a little bit more detail on why these amendments are needed for open banking.

Mr. Philippe Letarte: Of course.

I'm going to start with proposed section 18 on legitimate interests. Thank you so much, Mr. Williams, for introducing that bill. It really resonates and I think it really drives the point forward.

As you know, the purpose of open banking is to have consent and transparency. If we grant some exceptions.... I'm not against section 18 per se; I just think there should be at least some criteria or a definition of “exception”, because open banking is not about the use of secondary data. In that case, we could have some companies saying, “Yes, we have legitimate business interests,” and kind of breaking the confidence of consumers, because when you agree to share your data, you might not agree to share your data for secondary uses.

To that end, I believe we should have really clear criteria for exceptions to say what a legitimate interest is, because, as I mentioned, if we do not have trust in the system, open banking will not be a success.

We can also look to other legislation. In Europe, they are clearly explicit about what a legitimate interest is, and it's the same in Australia. There's language on which to base that, but I think it's really a confidence issue, and we should not let businesses decide which secondary uses are good.

On proposed section 72, it's because, with what was announced in the fall economic statement, it's important—and you mentioned it—that open banking be mandated in financial regulation. No one should be able to escape or abdicate their responsibility under the regime. They need to participate. It's kind of the network effect in business. We should be really careful with the wording we choose to make sure there's no competitive framework and that no stakeholder can escape their responsibilities.

This is why I come back to the simple notion that it's not “if”; it's “when”. When you enter that framework in which you are a participant, you have to obey the same rules everybody else does. That's kind of the notion of it. As I mentioned, every jurisdiction with successful customer-driven banking has a really strong imposition on banks.

Finally, the last one that I believe you wanted to know about was on clear interest.

● (1650)

Mr. Ryan Williams: That's proposed section 29.

Mr. Philippe Letarte: This is interesting also, because as with proposed section 18, we're not against it per se, but we should redefine the character of the consumer.

For example, if I'm a company and I'm offering a promotion that will give a better interest rate to a customer, should I get his consent by saying, “Hey, you're going to miss out on that promotion”? Technically it's in his best interests because it may be a lower interest rate, but in the same way, it's a business advantage for me, so we should clarify the exception in the criteria. There are also some use cases we see in the U.K. that are clearly defined.

For example, there is the case of the most vulnerable Canadians. If you take care of a senior person and you are their child, maybe the senior person is not able to consent to give their data away, but maybe you can work with a non-profit that will give you a clear indication of whether this person is being defrauded or there are unusual spending habits. If this person isn't able to consent at this time because they have a mental illness—Alzheimer's disease or anything else—we should have this exception really clearly defined in the criteria.

Again, we're not against it per se, but we should be careful about the kinds of exceptions we grant, because the premise of data portability rights is about consent.

[*Translation*]

The Chair: Thank you very much.

Mr. Gaheer, you have the floor.

[*English*]

Mr. Iqwinder Gaheer (Mississauga—Malton, Lib.): Thank you, Chair. Thank you to the witnesses as well for appearing before the committee.

My questions are for Monsieur Letarte.

I want to focus on proposed section 9 of the act, which we know requires each organization that's subject to the act to develop and maintain “a privacy management program that includes the policies, practices and procedures” it puts into place in regard to the obligations under the act.

Does your organization already have a management program in place?

Mr. Philippe Letarte: We don't. We are not client facing. I think this is important to say. We are basically a data aggregator. We create the pipes in the country from an application like Questrade or Wealthsimple to the banks.

It's something we believe every company should have. It's something we see, again, in every other jurisdiction that has an open banking regime. There should be a clear remedy and a clear section on a website or an app that says what remedies and what privacy programs are in place to protect the consumer.

If a consumer feels there was foul play and they need to be made whole, they can consult these policies in real time. It's also a way to unburden any tribunal or entity by making sure that the person checks with the company first.

As a privacy company, we do have one, but it's not as detailed as it should be. We encourage section 9 being put in place. We believe that every company participating in that ecosystem should have some form of remedy in place.

● (1655)

Mr. Iqwinder Gaheer: Do you believe this section is too onerous for organizations?

Mr. Philippe Letarte: I don't. I think it's appropriate.

Mr. Iqwinder Gaheer: How long do you anticipate it will take for Canadian firms to get in line with this new regulatory framework and to adapt to it?

Mr. Philippe Letarte: It depends. We're seeing astonishing growth in the U.K. Year over year, it's 80% growth. It's a really successful public policy.

As you know, open banking is in the news more and more. People are talking about it because people know about it. Also, an association that we're members of, Fintechs, made a campaign, and a lot of Canadians have signed up to the campaign, saying they need and want open banking. I think adoption for Canadians will be really quick. This is one of the reasons we need to move forward really rapidly with it; it's because there's clearly a need in the population.

I really believe that for four or five years, there's going to be super mainstream adoption.

Mr. Iqwinder Gaheer: My next question is for the witness panel generally, so it's for anyone who wants to take it.

We've heard witness testimony on this point before as well. It's with regard to the fact that there is a new tribunal. The tribunal, instead of the Privacy Commissioner, will directly impose those fines.

I want to get the impression of the witnesses on the panel.

[*Translation*]

Mr. Alexandre Plourde: Our views on the new personal information and data protection tribunal are mixed. On the one hand, it may be interesting to have a specialized tribunal with expertise in this area to make privacy decisions. On the other hand, we have reservations about the fact that this tribunal will have a lot of powers to review or overturn the office of the commissioner's decisions. Since the office of the commissioner is a body that can be trusted, in our opinion, the overturning of its findings should perhaps be avoided.

The fact remains that, for us, the basic problem is not so much the existence of this tribunal as the fact that the office of the commissioner can only recommend administrative monetary penalties. We believe that the office of the commissioner should have the power to impose them directly.

[*English*]

Mr. Iqwinder Gaheer: Don't you think the concentration of that power with just the Privacy Commissioner will be too much?

[*Translation*]

Mr. Alexandre Plourde: That is the model that has been adopted in Quebec for the Office de la protection du consommateur. A recent bill on planned obsolescence gives that body the ability to impose administrative monetary penalties directly.

I don't think that would give too much power to the office of the commissioner. Because of the spirit and the way the bill is designed, it gives non-compliant businesses multiple opportunities to comply with the act. The office of the commissioner's role includes providing information, but also establishing compliance agreements and having discussions with non-compliant companies to bring them into compliance with the act. It is really only as a last resort that the office of the commissioner should impose a monetary penalty. So I don't think we need to worry about that.

[*English*]

Mr. Iqwinder Gaheer: Thank you.

[*Translation*]

The Chair: Thank you.

Mr. Lemire, you have the floor.

Mr. Sébastien Lemire: Thank you.

Ms. Levac or Ms. Plourde, I have a quick question for you. We are talking about amending clause 107 of Bill C-27 to remove all restrictions on the exercise of consumers' right to pursue civil remedies. In your opinion, to what extent does that clause restrict the exercise of consumers' right to file a class action suit?

I think that's a fairly unique aspect that we haven't heard about at this table yet.

Mr. Alexandre Plourde: Thank you very much for your question. You said it was brief, but I have a lot to say.

● (1700)

Mr. Sébastien Lemire: Then it will be up to the chair to intervene.

Mr. Alexandre Plourde: The problem we have with clause 107 of Bill C-27 is that it threatens Quebeckers' right to pursue civil remedies, an issue that seems to have fallen off the radar in this bill, but that really worries us.

Based on this clause's current wording, the private right of action—the right to sue a company in a civil court under federal legislation—can only be exercised under very strict conditions: if the Office of the Privacy Commissioner of Canada has found that a company has failed to meet its obligations; if a compliance agreement has not made it possible to compensate the consumer; or if a fine has been imposed in one of the very specific cases set out in the bill.

Otherwise, the consumer cannot sue the company in a civil court, cannot sue for compensation, and cannot assert their rights in court. They could find themselves in a situation where the office of the commissioner, for example, did not accept the complaint they filed against the company or did not make a finding, thereby failing to meet the requirements set out in clause 107. The consumer would then be deprived of recourse in court and would not be able to sue the company in a civil court.

Option consommateurs is an organization that files class action lawsuits and pursues civil remedies before the courts. In many situations, it has launched class action lawsuits against tech giants. For example, it filed a lawsuit against Google. However, that class action lawsuit is not the result of a complaint handled by the office of the commissioner. If we had to interpret clause 107 of the bill strictly, such a class action lawsuit may not be able to take place.

As a result, in order to avoid endless constitutional debates before the courts, we ask that the legislator's intent be clarified, since it is not, I am sure, to limit remedies available to Quebeckers. To that end, we are asking that a subclause be added to clause 107 of Bill C-27 indicating that it does not exclude provincial civil law remedies. The provincial remedies, the civil remedies, would then be in addition to the remedies set out in clause 107. That would solve a lot of problems and legal debates for us and would give consumers a great deal of access to justice.

Mr. Sébastien Lemire: I'm out of time. Thank you.

The Chair: Thank you.

Mr. Masse, you have the floor.

[*English*]

Mr. Brian Masse: Mr. Chair, I apologize for leaving the room; I'm multi-tasking. There is only one of us here.

I hope this wasn't asked, but I think my colleagues will actually appreciate it. We'll go around the table again. Maybe we'll start this time in person.

Should political parties be part of this oversight included in the bill, or should they be excluded? I'd appreciate your opinion, and if you don't know, that's okay too. That's fine.

Mr. Philippe Letarte: I pass.

Mr. Brian Masse: Okay.

Voices: Oh, oh!

Mr. Brian Masse: Just so we can't—

Voices: Oh, oh!

[*Translation*]

Mr. Alexandre Plourde: As a consumer association, we don't deal with those kinds of issues. I just want to mention, however, that political parties are covered by the bill in Quebec.

The Chair: Mr. Gambs or Mr. Mellouli, if you want to weigh in, the floor is yours.

[*English*]

Mr. Sébastien Gambs: For me, I think it should also include political parties. Anyone who has to collect personal data should also be included in law. I mean, I come from France, where political parties are also subject to the privacy legislation, so I don't know why it should be different here. It's still sensitive and personal data, so the obligation should be the same for political parties.

Mr. Brian Masse: You're still going to get taxed the same, despite your position.

Do I have enough time—

Mr. Sehl Mellouli: [*Inaudible—Editor*]

Mr. Brian Masse: Oh, I'm sorry.

[*Translation*]

Mr. Sehl Mellouli: I agree with Mr. Gambs. I think political parties should be covered.

[*English*]

Mr. Brian Masse: Great. Thank you.

Thank you, Mr. Chair.

[*Translation*]

The Chair: Thank you, Mr. Massé.

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

Mr. Brad Vis: Thank you, Mr. Chair.

Ms. Levac, on October 3, Minister Champagne sent a letter to the committee indicating that the government is considering an amendment to the preamble of the bill and to section 12 of the Consumer Privacy Protection Act to enhance the protection of children's personal information.

In the brief you submitted to the committee, you state that the amendments proposed by Minister Champagne are not sufficient to adequately protect children's personal information. Today, in your testimony, you mentioned that we should make an amendment to the bill to protect the best interests of the child.

What other measures can we adopt to improve this bill in order to protect our children?

Ms. Sara Eve Levac: First, the proposed amendment to section 12 talks about the sensitivity of personal information that is collected, used or disclosed. There are other stages in the life of personal information where the best interests of the child should be taken into account, such as access to, retention of, or destruction of that information.

For us, the best interests of the child are part of a more global vision that makes it possible to take into account considerations other than the sensitivity of a piece of information, by asking questions about what is conducive to respecting all the rights of the child and its development.

In addition to the amendments that would incorporate the best interests of the child, we are also proposing an amendment to the French version of subclause 4(a). In the English version, it is clear that the child has the right to exercise their own recourse, but in French, it is less clear.

● (1705)

Mr. Brad Vis: Thank you.

I recently read about VTech and children's toys. Could we make an amendment to the bill to protect children when it comes to Internet-connected toys, among other things?

Ms. Sara Eve Levac: An amendment that takes into account the best interests of the child would force us to consider the best interests of the child in all stages of the design of a new toy, from its design to its marketing, and in all subsequent decisions related to a child's personal information.

Another way to protect children in relation to smart toys is the concept of privacy by design, which requires that privacy risks be considered in the design of a new service or good and throughout the process.

Mr. Brad Vis: Thank you very much.

In the brief you submitted to the committee, you state that the measures proposed in clause 55 of the bill enabling consumers to request the removal of their personal information are incomplete. You deplore the fact that the bill does not contain some iteration of a right to be forgotten, as is the case in Europe and Quebec.

What do you think are the shortcomings of clause 55?

Mr. Alexandre Plourde: Thank you very much for asking that question in French.

I have two things to say about clause 55.

First of all, as you mentioned, it provides for a right to delete, but with a caveat: If the company has stated in its policy that it can keep personal information, it will keep it. It gives a very broad way out for companies. A framework should be provided for this right to ensure that consumers are protected.

It's very important to be able to delete your personal information. In Quebec, there was the computer security breach at Desjardins, a financial institution that retained the personal information of its clients for a very long time. The ability to delete your personal information avoids harm and prevents identity theft.

However, the right to deletion provided for in the bill is not a right to be forgotten. In the digital environment, there is plenty of information about us that can be propelled into the public sphere, end up on corporate servers and remain there forever. The Internet never forgets. Even if the information is published legally, it can cause harm to consumers who are not affected by the right to disposal provided for in the bill.

For example, imagine that I am someone who committed a minor crime several years or several decades ago. If that pops up every time you Google my name, it can affect my job prospects, my reputation and my ability to rebuild my life. It's the same thing—

Mr. Brad Vis: It could even be a child who has done something stupid.

Mr. Alexandre Plourde: Yes, that's an even better example. When a child makes a blunder or someone else posts photos or videos involving them, all of that stays online indefinitely, and when you Google their name, it pops up. This can damage a person's reputation, cause them to be bullied, and even constitute material to commit identity theft.

Legislative solutions have been put in place. Europe has adopted the right to be forgotten, as we have done in Quebec. It's also called the right to de-indexing. It enables a person to go to Google or any other digital platform and ask them to remove certain personal information if they are being negatively affected.

● (1710)

Mr. Brad Vis: Has the Quebec bill ever been used? Do you have an example?

Mr. Alexandre Plourde: It's hot off the press; it just came into force a month or two ago, so I'm not aware of any enforcement cases.

Mr. Brad Vis: Okay.

If you find any, please let us know.

Mr. Alexandre Plourde: I'd be happy to.

The Chair: Thank you, Mr. Vis. I'm always happy to give you more time when you make the effort to speak in French. Congratulations, by the way. Your efforts have been noticed and are noteworthy.

Mr. Sorbara, you have the floor.

[*English*]

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

Philippe, in your opening remarks, you mentioned Australia as an example or as a bar. Hopefully, that's not a cap on anything that's done in terms of legislation.

Can you elaborate on how Australia has laid out its legislation and what you liked about the Australian model, please?

Mr. Philippe Letarte: Sure, absolutely.

Australia went beyond the financial sector and created a full customer data right. I mentioned that it includes telecommunication, but also energy and so on. Basically, it's a government-led model. It's led by the treasury, which is kind of like our own treasury. It's also mandated into three separate entities: the equivalent of the Privacy Commissioner, the equivalent of the competition and market authority, and another one which is in charge of the technical evolution of it, meaning everything about standards.

It's really a government-led model, in collaboration with the industry and some specific stakeholder groups. I think it's great, because it gives power and really great protection to the consumer.

Mr. Francesco Sorbara: What's your feeling about the guardrails in their model, if I can use that term?

Mr. Philippe Letarte: I think they're pretty accurate and complete. It's kind of the carrot-and-stick model. If you participate in the ecosystem, you can develop a business in a safe and secure way. However, if you do not, for example, stand up reliable APIs, if you don't confirm to privacy legislation, you first get important fines, but also you can be discredited in real time. You lose the privilege to participate in the model.

It really has consumers in mind, making sure that when they're doing business with a company, they can be sure that this business has the right validation and the right security and safety measures in place.

Mr. Francesco Sorbara: You mentioned the ecosystem. Any time that you update laws, rules, regulations and so forth after that hasn't been done for a 15-year or 20-year period, you want to have the regulations be principle-based—I like principle-based—so that they can expand with and adapt to evolving technology. It's a two-way street.

On the Australian model, since it's already been implemented, how was the ecosystem developed?

Mr. Philippe Letarte: I would say that it developed pretty well, and it's the same with the U.K. There is some form of accreditation. There are kind of tier accreditations. Basically, if you have a new model, instead of doing the full onerous process of joining and having the accreditation, you can go via an agent. It's also a safe and secure model.

The evolution is going well. Of course, technology is evolving quickly. They've made sure, as you mentioned, that it's principle-based, but they have the right committees or stakeholders who are firm about where they can exchange and move forward with the technology.

We were talking about open banking, but it's more and more about open finance and involving insurance, mortgages and wealth management as well. It's evolving in a good way, because they create this kind of environment where players who participate know that other accredited players are safe and secure and it's good doing business with them.

Mr. Francesco Sorbara: I'm a big proponent of open banking and I always have been. I've worked both on Wall Street and Bay Street. I try to keep up with everything that's happening within financial services. In open banking, there are different paths going on around the world, in the U.K., the European Union, Australia and the United States. We really need the update to these rules in order to take the next step on open banking.

Mr. Philippe Letarte: Absolutely.

Mr. Francesco Sorbara: My view has always been that the data belongs to the consumer.

Mr. Philippe Letarte: Absolutely.

Mr. Francesco Sorbara: We've rented that data out, basically, to get a service back from the company or entity that we're dealing with now.

● (1715)

Mr. Philippe Letarte: That's a nice way to put it.

Mr. Francesco Sorbara: Mr. Chair, I am finished.

[*Translation*]

The Chair: Thank you, Mr. Sorbara.

[*English*]

I summon you to your seat, Mr. Perkins. The floor is yours.

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

I want to start by following up on a couple of questions, one by the chair and one by Mr. Gaheer, my new lawyer.

Mr. Plourde, I'll start with the interesting question on the issue of blocking the tracking, which sort of struck me as you were saying it and as the chair was asking the question.

Is it a mechanism similar to the one we implemented a number of years ago, the do-not-call list? The government legislated that if you didn't want telemarketers and all those things calling, you could register there. I think it was a five-year thing. Is that a type of thing that the legislation here could do?

I'm struggling with how you could do it, because you're still dealing with having somebody.... If it's through cookies or through the cookie thing, which is very hard, as you mentioned, with the fatigue, it's very difficult to say that somebody will actually go through and click on “Do not track me” out of many options.

[*Translation*]

Mr. Alexandre Plourde: I like your analogy between the do-not-call list and a do-not-track list. I'll take it a step further. If I ask that my number be added to the do-not-call list, all companies must comply with my wish not to be called. I won't have to call each and every telemarketer to say that I don't want them to call me. We're proposing a similar principle for the digital sphere. The analogy makes sense.

I'll provide some context. When I browse the Internet, on almost any mobile application or technology company platform, I see my personal information being collected everywhere. Technology giants reuse that data for commercial purposes for targeted advertising, analyses and so on. Consumer consent for these practices is often not very effective. Most tracking websites use pop-up windows to ask consumers for their consent to data collection.

We're proposing that a parameter be built into the browser, for example, or into the telephone, that forces companies to comply with a person's decision to not have their personal information constantly collected. The industry has all kinds of mechanisms to help with this to some extent. For example, some mechanisms let us opt out of targeted advertising. However, they don't let us opt out of the ongoing collection of our personal information.

If I'm a consumer and I really want to stop my personal information from being collected online, one of the only options is digital self-defense. This means blocking cookies and downloading applications that block these systems. However, companies aren't legally obligated to comply with my decision to not have my information collected. We've been proposing to incorporate this obligation into the legislation for a number of years. This would solve the problem by making consumer consent effective and simple. It would be very accessible for consumers.

[*English*]

Mr. Rick Perkins: Thank you.

The next question I have I'll come back to. That's what I was seeking my legal advice on from Mr. Gaheer; it was on issues around the tribunal, so if I still have time, I'll come back to it.

Mr. Letarte, I think you mentioned issues around proposed subsection 29(1).

Mr. Philippe Letarte: Yes.

Mr. Rick Perkins: When I look at proposed subsection 29(1)—and thank you for bringing it up—it's under a heading of “Public Interest”, but it is pretty broad, and nowhere in the bill can I find a definition of “public interest”. I read it to mean that if you can't get consent in a timely way, you can still do whatever you need to do if it's in the public interest. That's the way I'm reading it.

I wonder if you could expand a little more on your thoughts on proposed subsection 29(1).

● (1720)

Mr. Philippe Letarte: Yes, of course.

Again, I find it a bit too broad. As an operator of a business, I think we should want some clarity on and criteria for what is in the public interest. We don't want to have a backlash from that, trying to create our own product where we find it doesn't fit the public interest, so I would welcome criteria and exceptions on clear public interest.

Again, there was the example I gave to Mr. Williams earlier. If I can benefit from a new program that will save me money automatically, but I have to commit by this deadline, is it in my clear interest? It probably is, because I'm going to save money, but is it also a commercial interest? Yes.

This is the kind of clarification that we want to have because, as I mentioned, the premise of open banking is about trust and being empowered with regard to your data so that you always know where your data is and you always know where there is consent. If suddenly someone is on board some program that he did not consent to or he is being sent direct marketing stuff that he did not consent to, this is not what the premise of open banking is, and this is, therefore, how you lose trust.

This is why we want clarification on what the public interest is, as well as exceptions and cases to show how we can navigate through that. Thank you for the question.

Mr. Rick Perkins: As a marketer, I'm always looking for those holes that I can drive a truck through to use data in any way I need to for the company I work for.

Voices: Oh, oh!

Mr. Rick Perkins: If I have time, Mr. Chair, I'll go to Mr. Plourde for my last question, based on my discussion.

I think we're all struggling here with the testimony we've had about the tribunal. Some people think it's a good thing. Some legal guys think it's a bad thing, for different reasons: Some think that there's too much power sometimes in a single person, a Privacy Commissioner, and not all Privacy Commissioners are created equal; others are saying that it will slow down the process, with others saying that it actually will speed it up because you don't have to go through the intricacies of the court directly from the Privacy Commissioner. Also, if you want to go to court after you don't like the tribunal, that's a more difficult thing, but it may actually speed it up or slow it down. The competition tribunal, for example, hasn't quite worked out to be as fast as people thought it would be.

You've made some comments, but I think we need a little more guidance on that one.

[*Translation*]

Mr. Alexandre Plourde: I think that you want to understand how the personal information and data protection tribunal affects consumer rights.

As I said earlier, we have mixed feelings about the personal information and data protection tribunal. We would rather the Office of the Privacy Commissioner of Canada have the power to impose administrative monetary penalties.

However, in our view, the personal information and data protection tribunal isn't the biggest issue. Our main concern isn't the tribunal. It's all the other common law courts where a consumer could bring proceedings against a company on the basis of the new federal privacy legislation. There's a major problem. The current bill contains a significant restriction that could undermine consumers when they want to use this legislation before the courts.

The issue isn't the personal information and data protection tribunal. The issue lies outside the criminal process, including the Office of the Privacy Commissioner of Canada and the new data protection tribunal. In our view, Bill C-27 seriously impedes, or at least threatens to impede, the civil process.

I'll talk about Quebec. It's the only area that we know well, obviously. Quebec has its own privacy legislation, which has more teeth than the legislation on the table today. Quebec also provides for civil remedies. If a company fails to meet its obligations under federal legislation, I can turn to the civil courts in Quebec to assert my rights.

We think that the current bill carries risks. We can't predict what the courts will say about the scope of section 107. We're worried that it could lead to long legal debates. We would like MPs to ensure that this bill doesn't interfere with civil remedies. We're very concerned about this issue. We urge you to take action to protect consumer rights in Quebec, in order to ensure that consumers can pursue remedies under this legislation, should the need arise.

The Chair: Thank you.

Mr. Van Bynen, you now have the floor for five minutes.

[*English*]

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

In previous testimony, and in some again today, there are two different approaches in managing and making safe the use of artificial intelligence.

The approach we're looking at currently is that we're looking at how we regulate artificial intelligence in various capacities. Those capacities are privacy, competitiveness and the use of technology.

Then we've heard in the past—and I think this was the reference in the previous meeting—about using the distributed model for regulation, which is to have the Privacy Commissioner take a look at the use of artificial intelligence in that capacity, and similarly to have the commissioner for competition and for technology do that as well.

My question is for Mr. Gambs.

What's your thought on those two different approaches? Which would you prefer, or which would you recommend as being more effective?

● (1725)

Mr. Sébastien Gambs: I think using the Privacy Commissioner's expertise on privacy and other issues in artificial intelligence is a good way to leverage the expertise that is already there. I think a centralized entity that is able to audit companies for privacy and also for fairness and explainability would be the more efficient way to go forward, rather than splitting this into different entities that would have to coordinate anyway, because this issue is intricate. If you are a machine learning engineer and you have to implement privacy, fairness and explainability in your AI model, there is tension and synergy between these issues, and you cannot do them separately. I think the auditing part would also be one entity with the expertise to do that.

Mr. Tony Van Bynen: Thank you.

My next question is for Mr. Mellouli.

You keep making references to the black box. First of all, you mentioned that it's critically important that we authenticate the data and ensure the data is accurate. One part of the question is, how do we go about making sure, or should we regulate a methodology for authenticating data?

Second, with respect to the black box that all of this goes into, the artificial intelligence and data act will impose the obligation on those responsible for the intelligence system to contribute to it. Is there a way to provide, or does this bill provide, sufficient algorithmic transparency, and is there enough authority in that in what you have seen in the bill? I'm concerned about the authenticity of the data and whether there is a way to regulate it.

Second is the transparency. Does the bill go far enough to satisfy the needs for the transparency of the algorithm?

Am I frozen? Can you hear me?

The Chair: Yes, Tony. You need to leave some time for translation.

[*Translation*]

Mr. Sehl Mellouli: I think that the bill, as it stands today, doesn't go far enough to regulate the black box. That's really the issue.

You're asking whether data use should be regulated. I think that it should. As you said a number of times, I think that the Privacy Commissioner can play a major role in raising awareness.

In all honesty, the data can be used for any purpose. I can give you any application. You click on the accept button and you're told that your request has been sent. As a consumer, you have no idea whether it has actually been sent. In the age of big data, managing hundreds of millions of data items is a complex business.

Will the bill make it possible to control everything? Personally, I'm not sure. It is possible to set out ways to train and educate people on data definitions, data selection and the use of data in artificial intelligence systems? I think so.

This can go beyond the data. It can even affect the teams that choose the data. This choice can have a major impact on discrimination. We've seen this in applications where certain categories of people weren't included in the data selection process. As a result, certain groups received positive treatment. However, one segment of the population received negative treatment. There are some examples of this issue.

In my opinion, the bill can be improved to better regulate data use; ensure greater accountability on the part of companies; and give the Privacy Commissioner a bigger role and more powers, by boosting the commissioner's ability to raise awareness and educate people about data use.

● (1730)

[*English*]

Mr. Tony Van Bynen: I have one quick question. Do you feel that there's enough value in the penalties?

I've read that there are monetary penalties. Is there any provision that should be considered in terms of requiring the offending party to disgorge the data that was created and/or to stop processing it? Do you feel that it would be a critical authority for the Privacy Commissioner or the tribunal to have?

If it's only a monetary penalty, then it simply becomes a cost of doing business. How can we have a more meaningful regime in terms of penalties?

[*Translation*]

Mr. Sehl Mellouli: There can always be a tougher penalty system. However, as I said earlier, these systems aren't foolproof. The flawed nature of these artificial intelligence systems must be taken into account. A company may comply with all the processes, but in the end, the results may not be consistent or expected. Also, when a company uses artificial intelligence data and sees hundreds of millions of data items, there's no guarantee that all the data is clean or compliant.

In my opinion, if restrictions on data use become much tighter, it could also hamper economic development. This ecosystem is developing at breakneck speed, and our companies must remain competitive. To that end, they need to use data. If data control is too restricted, it could slow down the development of systems. A smart system isn't developed overnight. It takes time.

As a result, data use must be controlled, but this control can't be exhaustive. There could be a form of supplementary control. This matters given that data lies at the heart of artificial intelligence. The more restrictions and reporting requirements are imposed on companies, the more it will adversely affect the economy. I don't know the extent of that impact. That said, global competition in this area is enormous.

The Chair: Thank you, Mr. Mellouli.

I think that you have hit the nail on the head when it comes to our concern. We need to strike a balance between these two interests, which don't always see eye to eye.

Mr. Lemire, the floor is yours.

● (1735)

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

Mr. Letarte, we heard that the bill doesn't clearly identify what qualifies as an adverse effect, particularly when it comes to exempting an organization with a legitimate interest from the need to obtain an individual's consent to collect, use and share their data.

In your expert opinion, how should the bill clarify this provision on adverse effects, and how could this ambiguity affect privacy?

Mr. Philippe Letarte: It's necessary to look at the reason for an adverse effect. A violation of privacy may be good for a company, but is it good for the consumer? There's always some sort of dilemma.

For example, a person's consumption habits can reveal very private information. For instance, these habits can show whether a person has started a diet, bought a house, cut back on spending or changed jobs. A company could get hold of this person's data to create a profile. The company could then notice that the person has changed their consumption habits and that they could benefit from new discounts. Technically, this would be a monetary benefit for the consumer. However, I personally don't think that it's good for a company to have that much information on a person.

The idea is to identify what qualifies as a positive or adverse effect using case studies. The consumer must always come first. When a company collects too much information on a person, it can become a major issue for them.

Mr. Sébastien Lemire: One adverse effect could be to conclude by association that the person is suffering from depression or has mental health issues.

I know that you like to look for innovative best practices. Could any best practices or models used in other places help clarify the provision on adverse effects connected to the legitimate interest exception?

Mr. Philippe Letarte: Yes. In Europe, the General Data Protection Regulation covers the entire continent and is extremely specific when it comes to legitimate interest. It also provides for various exemptions. It even establishes what qualifies as direct marketing and the circumstances that prohibit it. A number of bills determine whether highly targeted and relevant advertising can be deemed positive or adverse. Once again, Australia does more or less the opposite. It prohibits direct marketing, except in certain cases, and it clarifies these exceptions.

There are a number of good practices. The advantage of lagging behind the rest of the world in this area is that we can choose the approach that suits us best.

Mr. Sébastien Lemire: Thank you.

The Chair: Thank you.

Mr. Masse, the floor is yours.

[*English*]

Mr. Brian Masse: Thank you.

I'd like to continue with your opinions on the United States and its process right now. If we take a different approach, how will that potentially affect investment trading, because we have many companies that are matching up?

Thank you.

Mr. Philippe Letarte: The good news is that the CFPB released its first set of rules a couple of weeks ago, which closely look at what it wants to do. Of course, the CFPB doesn't care about everything and it takes more of a laissez-faire approach on some stuff, but for the first time, it clearly outlines that it wants to create a universal data protectivity right, and it's going to be imposed on financial institutions. Once that's done and we have the same approach—and I know people at Finance Canada are talking to people from the CFPB as well—I don't think it's going to be that difficult to do trade across the border, because the big team and the base principle are quite similar.

Mr. Brian Masse: Right. With that is more discretion for the consumer to choose the level of exposure that they want.

Mr. Philippe Letarte: Absolutely, and they can choose the time of exposure. For example, if you want to try two different companies for the same product and you prefer one of them, you can drop the other one immediately. Therefore, your data is not used by this company anymore.

It's really about the power of the consumer and the time in which you can revoke your consent.

Mr. Brian Masse: Thank you.

Thank you, Mr. Chair.

[*Translation*]

The Chair: Thank you, Mr. Masse.

This concludes the 100th meeting of the House of Commons Standing Committee on Industry and Technology.

I want to thank the panel. I'll take this opportunity to point out that meetings held in French to this extent in Ottawa are more the exception than the rule. Personally, I'm delighted that this was the case for the 100th meeting.

On that note, thank you. I also want to thank Mr. Mellouli and Mr. Gambs, who joined us virtually. I particularly want to acknowledge Mr. Mellouli, who is from Université Laval, in my constituency. I would also like to thank the interpreters, the analysts and the clerk.

We'll briefly suspend the meeting before continuing in camera for committee business.

The meeting is suspended.

[*Proceedings continue in camera*]