HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

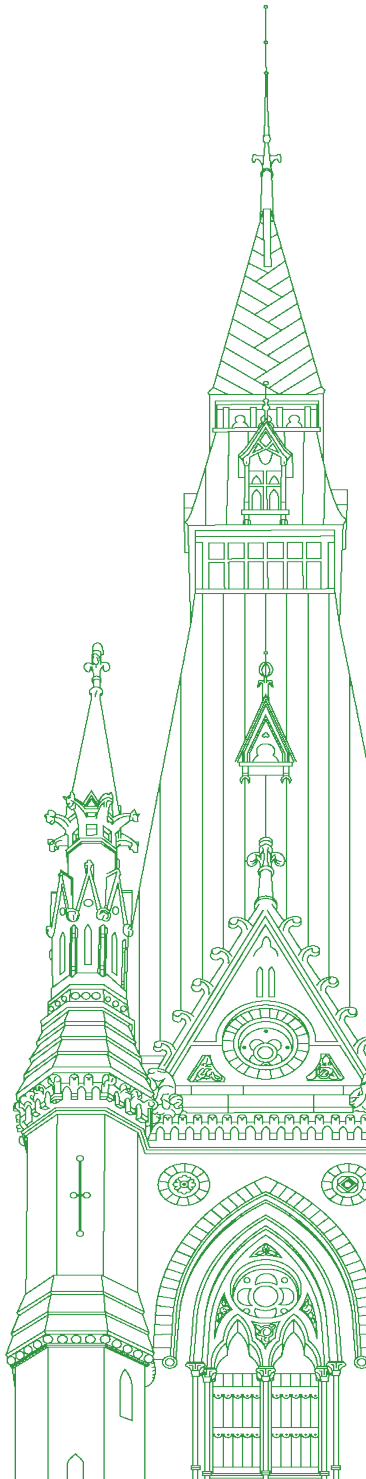
44th PARLIAMENT, 1st SESSION

Standing Committee on Industry and Technology

EVIDENCE

NUMBER 092

Thursday, October 26, 2023



Chair: Mr. Joël Lightbound

Standing Committee on Industry and Technology

Thursday, October 26, 2023

● (1545)

[*Translation*]

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

Welcome to meeting no. 92 of the House of Commons Standing Committee on Industry and Technology.

Today's meeting is taking place in a hybrid format, pursuant to the standing orders.

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

I'd like to welcome our witnesses today and also apologize for the brief delay caused by a vote in the House.

Joining us today are Colin J. Bennett, professor; Dr. Michael Geist, professor of law and Canada research chair in Internet and e-commerce law; Vivek Krishnamurthy, associate professor of law at University of Colorado Law School; Dr. Brenda McPhail, acting executive director of the public policy in digital society program; and lastly, Teresa Scassa, Canada research chair in information law and policy, Faculty of Law, Common Law Section, University of Ottawa.

I'd like to welcome you all.

We'll begin the discussion without further ado.

Mr. Bennett has the floor for five minutes.

[*English*]

Prof. Colin Bennett (Professor, Political Science, Unversity of Victoria, As an Individual): Thank you very much, Mr. Chair.

I'm from the University of Victoria, although I'm currently in Australia. I wish everybody a good day.

I would like to emphasize five specific areas for reform of the CPPA and to suggest ways in which the bill might be brought into better alignment with Quebec's law 25. I don't think that Bill C-27 should be allowed to undermine Quebec law, and in some respects, it does. I also think these are some of the areas where the bill will be vulnerable when the European Commission comes to evaluate whether Canadian law continues to provide an adequate level of protection.

Some of these recommendations are taken from the report that you have from the Centre for Digital Rights, which I'd like to commend to you.

First, I believe that CPPA's proposed section 15, on consent, is confusing to both consumers and businesses. In particular, I question the continued reliance on “implied consent” in proposed subsection 15(5), which states, “Consent must be expressly obtained unless...it is appropriate to rely on an individual's implied consent”.

The bill enumerates those business activities for which consent is not required, including if “the organization has a legitimate interest that outweighs any potential adverse effect on the individual”. That's a standard that has been imported from the GDPR. However, in the GDPR, “consent” means express consent; it's “freely given, specific, informed and unambiguous”.

In the current version of the CPPA, businesses can have it both ways. They can declare that they have implied consent because of some inaction that a consumer allegedly took in the past because of not reading the legalese in a complex terms-of-service agreement, or they can assert a “legitimate interest” in the personal data by claiming that there is no “potential adverse effect on the individual”. That is a risk assessment performed by the company rather than a judgment made about the human rights of individuals to control their personal information.

In that respect, it's really important that the bill be brought within a human rights framework. There should be no room for implied consent in this legislation. It's a dated idea that creates confusion for both consumers and businesses.

Second, there is no section in the CPPA on international data transfers. I find that very odd. I know of no other modern privacy law that fails to give businesses proper guidance on what they have to do if they want to process personal data offshore. The only requirement is for the organization to require the service provider, “by contract or otherwise,” to ensure “a level of protection of the personal information equivalent to that which the organization is required to provide under this Act.” That's proposed subsection 11(1) of the CPPA.

That due diligence applies whether the business is transferring personal data to another province in Canada or overseas to a country that may or may not have strong privacy protection or, indeed, a record of the protection of human rights. That's particularly troubling because of proposed section 19 of the CPPA, which reads, “An organization may transfer an individual's personal information to a service provider without their knowledge or consent.”

The Canadian government has never gotten into the business of adopting a safe harbour approach or a white list, and I'm not recommending that. However, Quebec, I believe, has legislated an appropriate compromise under section 17 of law 25, which requires businesses to do an assessment, including of the legal framework, when sending personal data outside of Quebec. As many businesses will have to comply with the Quebec legislation, why not mirror that provision in Bill C-27?

Third, the bill ignores important accountability mechanisms that were pioneered in Canada and exported to other jurisdictions, including Europe. Therefore, it's very strange that those same measures do not appear in the CPPA. In particular, privacy impact assessments are an established instrument and a critical component of accountable personal data governance, and they should be required in advance of product or service development, particularly where invasive technologies and business models are being applied, where minors are involved, where sensitive personal information is being collected, or where the processing is likely to result in a high risk to an individual's rights and freedoms. Businesses do the PIAs, and they stand ready to demonstrate their compliance or their accountability to the regulator.

A fourth and related problem is the absence of any definition of sensitive forms of personal data. The word “sensitivity” appears throughout the legislation in several provisions of the bill, but with the exception of the specification about data on minors, it is nowhere defined. In my view, the bill should define what “sensitive information” means, and it should also enumerate a non-exhaustive list of categories, which, in fact, occurs in many forms of legislation.

● (1550)

Finally—I know you've heard about this in the past, and I've researched on this—the absence of proper privacy standards for federal political parties is unjustifiable and untenable. The government is relying on the argument that the FPPs’ privacy practices are regulated under the Elections Act, but those provisions are nowhere near as strong as in Bill C-27. I think businesses resent the fact that parties are exempted. This is not an issue that will go away, given advances in technology and its use in modern digital campaigning. Canada is one of the few countries in the world in which political parties are not covered by applicable privacy law.

Thank you so much.

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

I'll now give the floor to Professor Geist, who is here with us in Ottawa.

Dr. Michael Geist (Professor of Law, Canada Research Chair in Internet and e-Commerce Law, Faculty of Law, University of Ottawa, As an Individual): Thank you very much, Chair.

Good afternoon. As you heard, my name is Michael Geist. I am a law professor at the University of Ottawa, where I hold the Canada research chair in Internet and e-commerce law and am a member of the Centre for Law, Technology and Society. I appear in a personal capacity representing only my own views.

I’d like to start by noting that the very first time I appeared before a House of Commons committee was in March 1999 on Bill C-54, which would later become PIPEDA. I must admit that I don't think I really knew what I was doing at that appearance, but my focus at the time was on whether or not the law would provide sufficient privacy protections for those just coming online who had little background or knowledge of privacy or security, or even the Internet, for that matter.

I highlighted some of the shortcomings of the bill, including poorly defined consent standards that would lead to overreliance on implied consent, broad exceptions on the use or disclosure of personal information and doubts about enforcement. I urged the committee to strengthen the bill, but I have to say that I did not fully appreciate that the policy choices being made back then would last for decades.

I start with this brief trip down memory lane because I feel that we find ourselves in a similar position today, with policy choices on things like artificial intelligence and emerging technologies that will similarly last for far longer than we might care to admit.

It is for that reason that I think it is important to emphasize the need to get it right rather than to get it fast. I often hear the minister talk about being first, at least on AI, and I must admit that I don’t understand why that is a key objective. Indeed, if you leave aside the fact that the core of at least the privacy part of this bill was introduced in 2020 and languished for years, we now find ourselves in a race to conduct hearings that I don’t totally get. We have an AI bill where there is a major overhaul with no actual text available yet. Witnesses seemingly have to pick between privacy and AI, creating the risk of limited analysis all around.

I think we need to do better. I'll focus these remarks on privacy, but to be clear, the AI bill and the proposed changes raise a host of concerns, including the need for independent enforcement and the high-impact definitions that puzzlingly include search and social media algorithms.

The other lesson from the past two decades is that you can seek to create a balanced statute—I know there's been a lot of talk about balance—but the playing field will never be balanced. It's always tilted in favour of businesses, many of which have the resources and expertise to challenge the law, challenge complaints and challenge the Privacy Commissioner. Most Canadians don't stand a chance. That's why we must craft rules that seek to balance the playing field, too, with broad scope of coverage, better oversight and audit mechanisms, and tough penalties to ensure that the incentives align with better privacy protection.

How do you do that? Given my limited time, I have five quick ideas.

First, to pick up where Professor Bennett ended, we must end the practice of "do what I say, not what I do" when it comes to privacy. I think it's unacceptable in 2023 for political parties to exempt themselves from the standards they expect all businesses to follow. Indeed, you can't credibly argue that privacy is a fundamental right and then claim that it should not apply in a robust manner to political parties.

Second, the addition of language around the fundamental right to privacy is welcome, but I think it should also be embedded elsewhere so that it factors more directly into the application of the law. For example, as former commissioner Therrien noted, it could be included in proposed subsection 12(2) among the factors to consider in an "appropriate purposes" test.

Third, the past 20 years have definitely demonstrated that the penalties matter for compliance purposes and are a critical part of the balance. The bill features some odd exclusions. There are penalties for elements of the appropriate purposes provision in proposed section 12, but not the main provision limiting collection, use and disclosure for appropriate purposes.

In the crucial proposed section 15 provision on consent, there are no penalties around the timing of consent or for using an implied consent within the legitimate interest exception. The bill says such a practice "is not appropriate", whatever that means. It is an odd turn of phrase in a piece of legislation. But the penalty provision doesn't apply regardless.

Fourth, the committee has already heard debate about the appropriate standard of anonymized data. I get the pressure to align with other statutes. I'd note that proposed subsection 6(6) specifically excludes anonymized data from the act, and yet I think we want to ensure that the commissioner can play a data governance role here with potential audits or review, particularly if a lower standard is adopted.

● (1555)

Finally, fifth, provided we ensure that the privacy tribunal is regarded as an expert tribunal that will be granted deference by the courts, I'm okay with creating another layer of privacy governance. I appreciate the concerns that this may lengthen the timeline for resolution of cases, but the metric that counts is not how fast the Privacy Commissioner can address an issue but how fast a complainant can get a binding final outcome. Given the risks of appeals and courts treating cases on a *de novo* basis, existing timelines can go far beyond the commissioner's decision, and the tribunal might actually help.

Thanks for your attention. I look forward to your questions.

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

We'll now turn to Professor Vivek Krishnamurthy. The floor is yours.

● (1600)

Mr. Vivek Krishnamurthy (Associate Professor of Law, University of Colorado Law School, As an Individual): Thank you, Mr. Chair and members of the committee. I am very honoured to be speaking with you today regarding Bill C-27.

I am currently a professor of law at the University of Colorado, but when I was the director of CIPPIC at the University of Ottawa, we published two reports in the spring of 2023 that consider AIDA and the CPPA. I am going to focus my remarks on the CPPA, particularly on provisions that relate to the privacy of minors. I would be happy to share some of my thoughts around AIDA as well.

I would like to begin by saying that I agree with everything that Professor Bennett and Professor Geist said. You could treat these remarks as additive.

While it is very welcome that the CPPA, unlike PIPEDA, specifically defines that the personal information of minors is sensitive information, Professor Bennett already told you about how "sensitive information" is not a defined term in the legislation. It is positive that children would have—if this bill passes into law—some recognition of the importance of protecting their personal information to a higher standard. However, we believe that this legislation can do far better.

For context, it is important to realize that children spend increasing amounts of time online, at younger and younger ages. This is a trend that accelerated during COVID-19 and the transition to digital online learning. I am a parent, and I am sure many of you are parents. Our children are using devices under commercial terms of service all the time, and this poses a very significant risk to the privacy rights of children.

While COVID has receded, it's the new reality that kids are using more and more technology at younger ages. What can we do? There are three things, and then a fourth about jurisdictional competence.

The Privacy Commissioner, in his recommendations regarding the CPPA, suggested that “best interests of the children” language should be incorporated into the law, and he suggested doing that in the preamble. I take no position myself as to where that should be done, but it is clear that this is international best practice. The United Kingdom and California have both incorporated such language into recently enacted statues, and we think that Canada should follow this approach. What would that mean? It means that organizations that handle children's personal data must take the best interests of children into account. That must come ahead of their commercial interests.

Second, we think it is important for the CPPA to require organizations that develop products or services that are likely to be accessed by children to set their privacy settings to the highest level. Defaults play a really important role in our subjective experience of privacy. It is great to have rights, but you can very easily leave those rights on the table if a setting is such that it contracts you out. We think that requiring a company to set those defaults to high levels when children are their likely users or their known users is very important.

Third, I'd like to pick up on what Professor Bennett told you about data protection impact assessments, a made-in-Canada idea. Bill C-27 is extremely weak when it comes to data protection impact assessments. The provisions apply only when the legitimate interest, excepting the consent, is being used. This is a problem for everyone, especially for children.

We believe—and I specifically believe this personally—that the data protection impact assessment requirements of this bill need to be considerably strengthened whenever data-processing activities pose a high risk to the privacy rights of Canadians. I would say that if children's data is sensitive data, that means we basically need to do that impact assessment all the time.

Last, I'd like to talk about constitutional competence here. There may be some concerns that it may be beyond federal competence to protect the privacy rights of children with more expansive provisions. Our analysis suggests otherwise. CPPA, like PIPEDA before it, is being enacted under Parliament's power to regulate trade and commerce.

Now, it is true that in our federal system, provincial governments get to determine the age of majority, but there is plenty of federal legislation that is designed to protect the rights of children. This also leads to how we think of this law, the consumer privacy protection act. It's not just a form of privacy regulation; it's also, when you think about it, a form of consumer protection legislation that is regulating the safety of digital products that invade and interfere with our right to privacy.

● (1605)

In view of the long history of federal regulation directed at protecting children in the marketplace, we think it would be appropriate for the federal government to include stronger privacy protections, and that would not prejudice provincial laws, like Quebec's, that are stronger. Just as PIPEDA yields to provincial legislation when it's substantially equivalent or better, the same could be true of strengthened children's privacy protections in the new CPPA.

Thank you very much.

[*Translation*]

The Chair: Thank you very much.

I will now turn the floor over to Dr. Brenda McPhail.

[*English*]

Dr. Brenda McPhail (Acting Executive Director, Master of Public Policy in Digital Society Program, McMaster University, As an Individual): Thank you, Mr. Chair and members of the committee, for inviting me here today to speak to the submission authored by Jane Bailey, professor at the faculty of law of the University of Ottawa; Jacquelyn Burkell, professor at the faculty of information and media studies at Western University; and myself, currently the acting executive director of the public policy and digital society program at McMaster University.

It is a privilege to appear before you on this omnibus bill, which needs significant improvement to protect people in the face of emerging data-hungry technologies.

I will focus on part 1 and very briefly on part 3 of the bill in these initial remarks, and I welcome questions on both.

Privacy, of course, is a fundamental underpinning of our democratic society, but it is also a gateway right that enables or reinforces other rights, including equality rights. Our written submission explicitly focuses on the connection between privacy and equality, because strong, effective privacy laws help prevent excessive and discriminatory uses of data.

We identified eight areas where the CPPA falls short. In these remarks, I will focus on four.

First of all, privacy must be recognized as a fundamental human right. Like others on this panel, while we welcome the amendment suggested by Minister Champagne, we would note that proposed section 12 in particular also requires amendment so that the analysis to determine whether information is collected or used for an appropriate purpose is grounded in that right.

Bill C-27 offers a significant improvement over PIPEDA in explicitly bringing de-identified information into the scope of the law, but it has diminished the definition from the predecessor law, Bill C-11, by removing the mention of indirect identifiers. The bill also introduces a new category, anonymized information, which is deemed out of the scope of the act, in contrast to the superior approach taken by Quebec. Given that even effective anonymization of personal data fails to address the concerns about social sorting that sit at the junction of privacy and equality, all data derived from personal information, whether identifiable, de-identified or anonymized, should be subject to proportionate oversight by the OPC, simply to ensure that it's done right.

Third, proposed subsection 12(4) weakens requirements for purpose specification. It allows information collected for one purpose by organizations to be used for something else simply by recording that new purpose any time after the initial collection. How often have you shared information with a business and then gone back a year later to see if it had changed its mind about how it's going to use it? At a minimum, the bill needs constraints that limit new uses to purposes consistent with the original consensual purpose.

Finally, the CPPA adds a series of exceptions to consent. I'll focus here on the worst, the legitimate interest exception in proposed subsection 18(3), which I differ from my colleagues in believing should be struck from the bill. It is a dangerously permissive exception that allows collection without knowledge or consent if the organization that wants the information decides its mere interest outweighs adverse impacts on an individual.

This essentially allows collections for organizational purposes that don't have to provide benefits to the customer. Keeping in mind that the CPPA is the bill that turns the tap for the AIDA on or off, this exception opens the tap and then takes away the handle. Here, I would commend to you the concerns of the Right2YourFace coalition, which flags this exception as one in which organizations may attempt to justify and hide their use of invasive facial recognition technology.

Turning to part 3 of Bill C-27, the AIDA received virtually no public consultation prior to being included in Bill C-27, and that lack of feedback has resulted in a bill that is fundamentally underdeveloped and prioritizes commercial over public interests. The bill, by focusing only on high-impact systems, leaves systems that fail to meet the threshold unregulated. AI can impact equality in nuanced ways not limited to systems that may be obviously high-impact, and we need an act that is flexible enough to also address bias in those systems in a proportionate manner.

A recommender system is mundane these days, yet it can affect whether we view the world with tolerance or prejudice from our filter bubble. Election time comes to mind as a time when that cumulative impact could change our society. Maybe that should be in, and maybe it should be out. We just haven't had the public conversation to work through the range of risks, and it's a disservice to Canadians that we're reduced to talking about amendments to a bad bill in the absence of a shared understanding of the full scope of what it needs to do and what it should not do.

Practically, in our submission, we nonetheless make specific recommendations in our brief to include law enforcement agencies in scope, to create independent oversight and to amend the definitions of harm and bias. We further support the recommendations submitted by the Women's Legal Education & Action Fund.

● (1610)

I would be very happy to address all of these recommendations during the question period.

Thank you.

[*Translation*]

The Chair: Thank you very much.

For the final speech, Teresa Scassa has the floor for five minutes.

[*English*]

Dr. Teresa Scassa (Canada Research Chair in Information Law and Policy, Faculty of Law, Common Law Section, University of Ottawa, As an Individual): Thank you very much, Mr. Chair, for the invitation to address this committee.

I am a law professor at the University of Ottawa, where I hold the Canada research chair in information law and policy. I'm appearing today in my personal capacity.

I have concerns about both the CPPA and the AIDA. Many—

[*Translation*]

Mr. Sébastien Lemire (Abitibi—Témiscamingue, BQ): Mr. Chair, I must intervene to advise you that we have no interpretation.

[*English*]

The Chair: Okay.

Wait just one minute, Ms. Scassa.

We'll make sure the interpretation is working.

[*Translation*]

Mr. Sébastien Lemire: It's working now.

Thank you very much.

[*English*]

The Chair: Amazing. You can now resume.

Dr. Teresa Scassa: Thank you.

I have concerns about both the CPPA and the AIDA. Many of these have been communicated in my own writings and in the report submitted to this committee by the Centre for Digital Rights. My comments today focus on the consumer privacy protection act. I note, however, that I have very substantial concerns about the AI and data act, and I would be happy to answer questions on that, as well.

Let me begin by stating that I am generally supportive of the recommendations of Commissioner Dufresne for the amendment of Bill C-27, as set out in his letter of April 26, 2023 to the chair of this committee.

I will address three other points.

The minister has chosen to retain consent as the backbone of the CPPA, with specific exceptions to consent. One of the most significant of these is the "legitimate interest" exception in proposed subsection 18(3). This allows organizations to collect or use personal information without knowledge or consent if it is for an activity in which an organization has a legitimate interest. There are guardrails: The interest must outweigh any adverse effects on the individual; it must be one that a reasonable person would expect; and the information must not be collected or used to influence the behaviour or decisions of the individual. There are also additional documentation and mitigation requirements.

The problem lies in the continuing presence of "implied consent" in proposed subsection 15(5) of the CPPA. PIPEDA allowed for implied consent because there were circumstances where it made sense and there was no legitimate interest exception. However, in the CPPA, the legitimate interest exception does the work of implied consent. Leaving implied consent in the legislation provides a way to get around the guardrails in proposed subsection 18(3). An organization can opt for the implied consent route instead of legitimate interest. It will create confusion for organizations that might struggle to understand which is the appropriate approach. The solution is simple: Get rid of implied consent. I note that implied consent is not a basis for processing under the GDPR. Consent must be expressed, or processing must fall under another permitted ground.

My second point relates to proposed section 39 of the CPPA: an exception to an individual's knowledge and consent where information is disclosed to a potentially very broad range of entities for "socially beneficial purposes". Such information need only be de-identified—not anonymized—making it more vulnerable to re-identification. I question whether there is social licence for sharing de-identified rather than anonymized data for these purposes. I note that proposed section 39 was carried over verbatim from Bill C-11, when "de-identified" was defined to mean what we now understand as anonymized. Permitting disclosure for socially beneficial purposes is a useful idea, but proposed section 39, especially with the shift in meaning of "de-identified", lacks necessary safeguards.

First, there is no obvious transparency requirement. If we are to learn anything from the ETHI committee's inquiry into PHAC's use of Canadians' mobility data, transparency is fundamentally important. At the very least, there should be a requirement that written notice of data sharing for socially beneficial purposes be given to the Privacy Commissioner of Canada. Ideally, there should also be a requirement for public notice. Further, proposed section 39 should provide that any sharing be subject to a data-sharing agreement, which should also be provided to the Privacy Commissioner. None of this is too much to ask where Canadians' data are conscripted for public purposes. Failure to ensure transparency and a basic measure of oversight will undermine trust and legitimacy.

My third point relates to the exception to knowledge and consent for publicly available personal information. Bill C-27 reproduces PIPEDA's provision on publicly available personal information, providing in proposed section 51 that "An organization may collect, use or disclose an individual's personal information without their knowledge or consent if the personal information is publicly available and is specified by the regulations." We have seen the consequences of data scraping from social media platforms in the case of Clearview AI, which used scraped photographs to build a massive facial recognition database. The Privacy Commissioner takes the position that personal information on social media platforms does not fall within the "publicly available personal information" exception.

Not only could this approach be upended in the future by the new personal information and data protection tribunal, but it could also easily be modified by new regulations. Recognizing the importance of proposed section 51, former Commissioner Therrien recommended amending it to add that the publicly available personal information be "such that the individual would have no reasonable expectation of privacy." An alternative is to incorporate the text of the current regulations specifying publicly available information into the CPPA, revising them to clarify scope and application in our current data environment. I would be happy to provide some sample language.

This issue should not be left to regulations. The amount of publicly available personal information online is staggering, and it is easily susceptible to scraping and misuse. It should be clear and explicit in the law that personal data cannot be harvested from the Internet, except in limited circumstances set out in the statute.

● (1615)

Finally, I add my voice to those of so many others in saying that data protection obligations set out in the CPPA should apply to political parties. It is unacceptable that they do not.

Thank you.

The Chair: Thank you, Professor Scassa.

Before I open the discussion to Mr. Williams, I think I speak on behalf of the committee in asking you, if you could, to provide that language to improve proposed section 51 to the committee. It would be much appreciated.

Mr. Rick Perkins (South Shore—St. Margarets, CPC): Great.

The Chair: Then Mr. Perkins won't have to ask for it.

Mr. Rick Perkins: That will save four minutes.

The Chair: Mr. Williams, the floor is yours.

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

After eight long years, we finally have privacy legislation in front of this committee. Of course, we've heard from witnesses that it's actually been 24 years since we updated the last privacy legislation.

When we looked at this at second reading in the House, we really focused on what was missing in this bill. What was missing was listing privacy as a fundamental right. However, when we came to committee and we had witnesses lined up, the minister added a bunch of amendments. The amendments seemed to indicate that he was listening. Of course, we're not sure where we are, because amendments will go in certain parts of the bill.

Mr. Geist, thank you for appearing today. When we had the original copy of this, I understand you were part of the original iteration of this bill, PIPEDA, 24 years ago. You don't look that old, sir.

The minister came and presented a bill and did not list privacy as a fundamental right, and now there are all these amendments. Did the minister break this bill?

Dr. Michael Geist: When the minister first came to committee and suggested a whole raft of changes, and then indicated that the government was not prepared to provide the actual text of those amendments until clause-by-clause, to me, that broke the hearings. It broke them for my fellow witnesses and for the many witnesses to come. We follow closely.... The idea that you can come before a committee and comment intelligently when you don't have the actual text of the legislation means to me that everybody's time is being wasted a bit, because you're basically commenting on an old bill, rather than where things are headed.

I'm glad there are now some amendments there, but obviously we're carrying on. We don't have the specific language around the AIDA. Also, as I mentioned in my opening remarks, even around the issue of the fundamental right to privacy, I think we can still do better.

Mr. Ryan Williams: For the record, sir, do you believe that privacy should be listed as a fundamental right in the first two sections of this bill?

Dr. Michael Geist: I do. I think that would provide clarity in how it is interpreted by the commissioner, obviously, as well as by the courts, and it would provide a strong signal from the legislative branch of the importance it accrues to privacy.

However, as I mentioned, in many respects, I'd love to see this in some core provisions that are ultimately going to serve as a testing ground when there's analysis, when you make the determination, for example, of whether consent is appropriate or whether it is for the appropriate purpose. That's when you can begin to bring in that privacy is a fundamental right, because at that stage, you're engaged a bit in some of that balancing, rather than the more overarching side, which, it seems to me, may come at a later date. A court is reviewing a decision. Did the commissioner take adequate account of the fact that privacy has that elevated status?

Mr. Ryan Williams: Speaking of how important this is for all sections, you were involved 24 years ago in the first iteration—I'm sorry. I'm going to keep repeating that.

How hard is it, once we enact this legislation, to reverse or update it?

● (1620)

Dr. Michael Geist: I must admit that I'm genuinely surprised at how hard it becomes. I think part of it is because, as you will see throughout the course of these hearings, you end up with people coming from all different perspectives. This isn't a big political winner. I don't get that sense. I think it's critically important legislation, but it's not the thing that is seen as necessarily driving votes, so it tends to slip. We've seen it with this legislation.

Even with PIPEDA, with a mandatory five-year review, we got that first review after five years and it took years before those recommendations were acted on. We have never really seen an effective subsequent review since.

I think it's fairly clear that whatever choices are made now, you need to be prepared to say you're comfortable that these will be the rules in 2035, or maybe even in 2040. That means doing your best to get it right and not doing your best to get it fast.

Mr. Ryan Williams: On that note, we have a third section here. It seems to be hastily put together. It seems we didn't have public consultation.

Is it in Canada's best interest to be first out of the gate on AI legislation?

Dr. Michael Geist: It's in Canada's interest to get right what is a critically important issue—appropriate regulation of artificial intelligence. The idea that we want to race ahead with no consultation is just the wrong way to do something that all Canadians have an active interest in. We saw the government do the same on the generative AI guardrails, which were conducted privately, in secret, over the summer, and then rushed out with practically no public discussion.

When we look at some of the developments taking place around the world, we see that it becomes essential in terms of the kinds of protections Canadians might get with AI systems as well as some of the economic interests driven by the adoption of AI. We want to ensure that we contribute to that global conversation, and that some of our rules are broadly consistent with where things are headed, provided that they meet the kinds of standards that we're looking for.

In this instance, it's hard to figure out what the government is doing, other than that it raced out a sort of skeleton piece of legislation, got criticized for the lack of consultation and the lack of detail, and now says, “Okay, we'll provide more detail that makes it look a little bit more like Europe”, but we don't even have the language on that yet either.

Mr. Ryan Williams: I'm going to ask you a broad question—fundamental, though.

Who owns Canadians' data?

Dr. Michael Geist: We, as individuals, of course, ought to be the ones who own and certainly control our own data. That doesn't mean we can't make decisions about how organizations use that information, but what it requires is legislation that ensures we have that effective control, that it's informed—you heard several witnesses talk about the problems with things like implied consent—and that there are real penalties when organizations run afoul of what they've committed to Canadians or to the law itself.

Mr. Ryan Williams: Thank you, Mr. Geist.

The Chair: Thank you very much.

[*Translation*]

Mr. Gaheer now has the floor for six minutes.

[*English*]

Mr. Iqwinder Gaheer (Mississauga—Malton, Lib.): Thank you, Chair.

Thank you to all the witnesses for making time for the committee, and for their testimony.

My questions are for Ms. McPhail.

In the brief that you co-authored and submitted to the committee, you recommended that Bill C-27 be amended to “Ensure continued and appropriate protection of de-identified and 'anonymized' information”. We spent our last committee meeting on Monday with witnesses who talked about the definition maybe being too stringent, the fact that we've raised the bar too high.

What are your concerns regarding the protection of de-identified information and of anonymized information in the CPPA, and how can it perhaps be amended to address your concerns?

Dr. Brenda McPhail: I think there will always be differences of opinions as to whether definitions are sufficiently stringent or overly weak.

What would address our concerns? There are three categories of concerns that we have around de-identified and anonymized information. The first is that the definition has been weakened between Bill C-11 and the current iteration, Bill C-27. In the past definition, it included indirect identifiers. You can identify me by my name, but you can also identify me if you have a combination of my postal code, my gender and a few other factors about me. To truly de-identify information to an adequate standard where re-identification is unlikely, I believe—and my co-submitters believe—that the definition should include indirect identifiers.

To some degree, that definition has been weakened because Bill C-27 includes the addition of a new category of information: anonymized information. The problem with that new category is that technically people agree that it's extremely difficult to achieve perfect and effective anonymized information, and by taking anonymized information out of the scope of the bill, what we do is remove it from the ability of the Office of the Privacy Commissioner of Canada to inspect the processing that has happened to ensure that it has been done to a reasonable standard.

Like some of the witnesses you heard from—who would disagree with me about whether or not definitions should be stronger or weaker—I think we all agree on the reality that when personal information is processed, whether it is used to create de-identified information or anonymized information, there should be some checks and balances to make sure that the companies doing it are doing it to a reasonable standard that is broadly accepted. The way to achieve that is by including the ability within the bill for the Office of the Privacy Commissioner to inspect that processing and give it a passing grade, should that be necessary.

The last piece of concern we have with anonymization, which makes that scrutiny even more important, is that the bill conflates anonymization with deletion. It was introduced to great fanfare when this bill was put forward that individuals would now have a right to request deletion of their personal information from the companies with which they deal.

That right, I believe, is rendered moderately illusory. Certainly members of the public would not expect that if they ask for their information to be deleted, an organization could say, yes, they'll do that, and then simply anonymize the information and continue to use it for their own purposes. If we are going to allow anonymized information to be equivalent to deletion, again, it's incredibly important that we are 100% certain that the equivalency is real and valid, that truly no individual can be identified from that information and that it's not going to harm them in its use after they've explicitly exercised their right to ask for deletion.

● (1625)

Mr. Iqwinder Gaheer: Are you saying that there are levels to how anonymized data can be? If it's de-identified or anonymized, that would imply that you can't identify the person from it. Are you saying that even after meeting the bar of what this legislation puts forward, there are companies or individuals who can piece that together to find out the identity of that individual?

Dr. Brenda McPhail: Roughly speaking, de-identified information should make it highly unlikely that an individual can be identified. Anonymization should make it impossible. However, there are really important technical conversations happening about whether it's truly possible in our big data age, where we have data brokers who advertise that they have thousands of data points on up to two million or two billion people, that some recombination of data wouldn't facilitate re-identification. It's unlikely. It's not a risk that should be at the top of our consideration, but it should be there.

If this bill is to provide appropriate protection for people, ensuring that the technical standards of anonymization.... Computer science is a changeable field, and these standards change over time. Ensuring that someone has the oversight to ensure that the standards being used are appropriate in the circumstances is fundamentally important.

Mr. Iqwinder Gaheer: Thank you.

Chair, how much time do I have left?

The Chair: You're out of time, Mr. Gaheer, but I'm willing to let you go if you have one short question.

Your questions are good.

Mr. Iqwinder Gaheer: This is not a short question. It's about the exemptions to consent.

I know the witnesses talked about the “legitimate interest” exception. Quickly, I will shorten the question down.

I don't think that without that exception we would have things like Google Street View, so I want to get Ms. McPhail's view on the “legitimate interest” exception, because I think that without that you can stifle innovation in unforeseen ways.

Dr. Brenda McPhail: I think it's an interesting question about the way the “business activities” exemption and the “legitimate interest” exemption can interact, along with the question of implied versus explicit consent. It's very difficult to answer this question in a few seconds.

Broadly speaking, if we are to allow organizations to decide whether or not it's in their legitimate interest, then at a minimum we need to enhance the accountability and transparency measures, so that it doesn't happen without the knowledge or consent of individuals, and there is a requirement for organizations to justify to the public why they believe this information is in their legitimate interest to collect, and how they're protecting it.

● (1630)

[*Translation*]

The Chair: Thank you very much.

[*English*]

Thank you, MP Gaheer.

[*Translation*]

Mr. Lemire now has the floor.

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

I'd like to thank all the witnesses.

Mr. Bennett, in your February 12, 2021, submission to the public consultations on Bill C-11, you distinguished between the concepts of interoperability and harmonization. I believe this is particularly germane to the subject before us, because these two concepts can be confused. You showed the difference between the two with an example I'd like to quote:

> For instance, the processes for doing PIAs should be interoperable between the federal government and the provinces. If an organization does a PIA under the authority of one law, it may need the assurance that the PIA will also be acceptable in another jurisdiction. But that does not necessarily mean the harmonization or convergence of rules.

First, can you provide us with a definition of these two distinct concepts?

Second, can you tell us whether the provisions of Bill C-27 promote the interoperability of processes among the various levels of government or rather the harmonization of rules?

[*English*]

Prof. Colin Bennett: Thank you for that question.

I was trying to draw, in that statement, a distinction between harmonizational convergence, which is a harmonization of text ensuring that the statutes essentially say the same thing, and interoperability, which I think means something subtlely different. It means that if businesses have a requirement to do something in one province or one jurisdiction, such as a privacy impact assessment under Quebec's law 25, it will in fact be accepted by a regulator elsewhere. You can see that distinction in Canada among different provincial laws that have been worked out over time pragmatically, but it's also important to see it internationally through the GDPR.

That was the point I was trying to make. I'm not an expert on Quebec law, but I was trying to point out certain areas in Quebec's law where I think businesses would be required to do more under that law than they would under the current text of Bill C-27. Then you have to ask this question: What might be the economic impact of that across Canada if the CPPA is perceived to be lowering the standard within the Quebec legislation? That's the point I was making.

I think the particular provision on international data flows is an interesting example, because in the CPPA at the moment there's really nothing explicit for businesses on what to do when they are processing data offshore, and the vast majority of data protection laws that I know of.... This is also something that's of critical importance to the European Union when it comes to making a judgment about the adequacy, and the continued adequacy, of our laws in Canada. What happens when data on Europeans comes to Canada and then it is processed offshore elsewhere? Those are critical questions. I think there would be some concerns about that by our European friends when they come to make those judgments.

I hope that answers your question.

[*Translation*]

Mr. Sébastien Lemire: Thank you very much.

With respect to the shortcomings of the Canadian law, in an article entitled “What political parties know about you”, one thing you talk about is the factors affecting how political parties, MPs or independent candidates protect the personal information of Canadians that they may have in their possession. In the current context, Bill C-27 makes no mention of protection of this kind.

Is the government falling short of protecting voter data and perhaps moving forward in the quest for open and transparent governance?

Do you think Canada should follow Quebec's lead and subject federal parties to the same privacy standards as organizations?

[*English*]

Prof. Colin Bennett: Thank you for reading that work.

I first wrote about this issue about 10 years ago, when I issued a report to then commissioner Stoddart on political parties and privacy. It was obvious back then that there was a major gap in our law. Then Cambridge Analytica came along, and the issue hit the front pages, and there was a lot more attention to this.

I'll say this. It's become increasingly indefensible and untenable for political parties to be exempted—to say that they're exempted, to be clear—from provisions that businesses have to comply with, and I don't think the issue is going to go away.

The question is how that is done. An easy thing to do would be to apply the CPPA to federal political parties. That wouldn't necessarily undermine what Quebec has done, although the Quebec law, in fact, is an amendment to your Elections Act. It's by no means as far as I would want to go.

In British Columbia, the commissioner's office there has made a ruling that, in fact, that law does apply to federal political parties, as well as provincial political parties. That ruling is currently under judicial review, but you do have a real problem of interoperability, to go back to your original question, meaning that it's become absurd that the provincial political parties should have to comply with a higher set of standards in B.C. and Quebec than federal political parties federally.

I don't think that's in the interest of our political parties, either. It needs to be fixed. There need to be standards for federal political parties to comply with commonly accepted privacy standards of the kind that we are debating here with respect to businesses.

● (1635)

[*Translation*]

Mr. Sébastien Lemire: Thank you very much for your answer.

The Chair: Thank you, Mr. Lemire.

Mr. Masse, you have the floor.

[*English*]

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

I apologize to our guests for being a little bit late. Our Conservative colleagues were up to mischief in the House today delaying things.

Some hon. members: Oh, oh!

Mr. Brian Masse: I'm just kidding.

If I ask a couple of questions that are a little out of context, I apologize.

I'd like to start with Mr. Geist.

With the Privacy Commissioner, one of the proposed changes is the creation of a tribunal. I'm just wondering if you have any thoughts about that. I have mixed emotions on it and thoughts, subsequent to that.

I've also seen recently what the tribunal has done to the Competition Bureau, and I'm really worried that we could be in the same boat. I was told by administrative people from the department that it couldn't happen, but others are now telling me that it can happen. I'm in a bit of a vacuum of space here, and I would like your opinion on that situation.

Dr. Michael Geist: I did highlight that in the opening remarks, but I'm happy to engage.

You're right. When we look at what we just saw most recently involving Rogers and Shaw, it's understandable why people would be skeptical about the creation of a tribunal that provides that kind of oversight.

With that said, one of the things we have seen over the years is that, because of the way the federal court treats Privacy Commissioner decisions on a *de novo* basis—if there are appeals, they go to the court, and the court then effectively starts from scratch—you are faced with a situation where it almost incentivizes challenging tough cases—and we've seen that—because you get another chance at it.

Creating a tribunal, provided it is viewed from an administrative law perspective as an expert tribunal that's going to be granted some deference for the decision by follow-on courts, if it does go to court, has the potential, in some ways, to strengthen the outcomes of that process, because there is some of that deference, but that requires ensuring that the tribunal is genuinely viewed as an expert tribunal and properly constituted.

The initial version of this bill didn't go anywhere near there, with just one privacy expert. We now have half.

Finding ways to ensure that public interest is well represented on the tribunal and that the tribunal has genuine expertise at least opens the door to the prospect that it might provide some advantages, although I recognize why some would say that these are already lengthy processes so we should just let the Privacy Commissioner handle it all.

● (1640)

Mr. Brian Masse: Let me see if I have the summary of this right.

If we create a tribunal that is respected by the industry across the board, it might provide a better path to go forward. If it's not, it's going to lead to an opening for an initial test drive, in order to see whether we bring things to court.

I'm sorry. I'm trying to figure this out.

Dr. Michael Geist: It's not whether or not business respects the tribunal. I don't really care if business respects the tribunal.

Mr. Brian Masse: Okay, that's fair enough. That's why I'm asking.

Dr. Michael Geist: I think it should be properly constituted and recognized as a credible authoritative tribunal. However, the question isn't whether or not business respects it. It's whether or not courts respect it.

Mr. Brian Masse: Okay.

Dr. Michael Geist: What we want is for the courts to say that a decision that comes out of the tribunal is one they are prima facie going to respect.

At the moment, when the commissioner issues a decision, the courts start from scratch. They have the ability to start from the beginning, which is why we see.... The case of Cambridge Analytica has already been referenced a couple of times today. We still have Cambridge Analytica before the Canadian courts. We had the commissioner, then we had a first court decision, and now we have an appeal ongoing.

These are long processes and the courts play out potentially somewhat differently than the administrative side in terms of privacy itself. It's more about having the process of the Privacy Commissioner and the tribunal better respected by courts, especially given the kinds of penalties we're envisioning. I think we can well assume that, if the penalties are significant, we're going to see organizations that are facing those penalties appealing the decision through the courts.

Mr. Brian Masse: Okay.

I've had a lot of confidence in a number of the last privacy commissioners we've had. However, if the tribunal is going to be politically appointed, and if it's not respected by the courts, then I see what you're saying, because their decision-making capability and evaluation will be based on the confidence the groups going through the complaint have in the process.

Dr. Michael Geist: I'm not an administrative law expert, but the way a mistrial works, in terms of the deference courts may give to tribunals, is linked to the expertise of a tribunal. Let's say it's the copyright context. It doesn't mean the decisions themselves are always followed. They're definitely not, but at least the starting point is that they recognize there has been expertise brought to bear.

Right now, however, even though I think we would all acknowledge the Privacy Commission has expertise, it's not viewed as an independent tribunal. Thus the courts have taken the position that they have the ability to start looking at a case from the beginning.

Mr. Brian Masse: Okay, that's very helpful.

I know we have some guests online. I don't want to shut them out. To any of the guests online, please intervene. Is anybody interested in commenting on the creation of the tribunal for the Privacy Commissioner?

Please go ahead.

Dr. Teresa Scassa: Do you mean me?

Mr. Brian Masse: Yes. I'm sorry. It's hard for us to see. Raise your hand or just pipe up. It's all good.

Thank you.

Dr. Teresa Scassa: I am less enamoured with the proposed privacy tribunal, for a number of reasons.

The first thing is that.... It's certainly true that the Federal Court, under the section 14 process in PIPEDA, specifically in the legislation, holds its hearings *de novo*. You can change that. You can keep the same framework, but you can require that it not be a proceeding *de novo*. It is currently part of the legislation, but that part could be changed without creating a whole new data tribunal.

Currently, the Privacy Commissioner doesn't make decisions. They don't have order-making powers. The commissioner makes findings. The process before the Federal Court is a process where either the commissioner or the complainant seeks an order, or the complainant is seeking damages. It's not an appeal proceeding. The organization, for example, doesn't have a mechanism through that process to go to the court. Again, you could certainly tinker with that formula, but it isn't really an appeal; it's a hearing *de novo* on this issue of whether an order should issue.

With the personal information and data protection tribunal, the tribunal is actually going to now have the authority not only to review orders of the Privacy Commissioner—because the commissioner will have new order-making powers—or to review recommendations for administrative monetary penalties, but also to hear appeals of any findings, because the commissioner can still make findings. Findings aren't orders. They're not binding. They're the commissioner expressing particular views about the law. Those can also be appealed to the tribunal.

I think that requires another look in this context. Really, what you're doing is taking an independent regulator with the approach and interpretations that the independent regulator brings to their decision-making role. You then have an appointed tribunal that is going to review those decisions and findings, those approaches and interpretations that are not binding and that are the commissioner's approach to the law.

One of the things I've expressed concerns about.... The previous commissioner and the current commissioner have been working very collaboratively with the provinces that have private sector data protection laws, so Alberta, B.C. and Quebec. They have engaged in joint investigations. They have issued joint findings. They work in a way that is very collaborative to try to ensure some sort of consistency across the country with respect to interpretations of their laws, and to try to find cohesive shared interpretations of the laws.

We're going to move into a situation where the commissioner has less latitude, because the commissioner may agree with the provincial commissioners, who have order-making powers and are only subject to judicial review and not appeal before any kind of tribunal. The federal commissioner will perhaps agree with them in joint findings and then find those findings appealed to a tribunal that might rule otherwise, disrupting that collaboration among commissioners and the balance that might be found there.

I have quite a number of concerns about the tribunal structure and what implications it might have for how decisions are made about the interpretation and application of the legislation.

● (1645)

Mr. Brian Masse: That's great. Thank you very much.

Thank you, Mr. Chair.

[*Translation*]

The Chair: Thank you very much.

[*English*]

Mr. Vis, the floor is yours.

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

Thank you to our witnesses here today.

I'm somewhat concerned about this bad bill before us today.

With Bill C-11, the Government of Canada had an opportunity to enshrine the fundamental right to privacy for children, to define what a minor is, to define perhaps an age of consent and do a whole bunch of stuff to ensure that children were protected. That bill died on the Order Paper.

Then, we had Bill C-27 when this Parliament opened up again. The minister again had an opportunity to enshrine the fundamental right for children to protect their privacy in some of the actions they may take online. Then the government had the opportunity to define what sensitive information is—likely in the context of a child. They had an opportunity to define what a socially beneficial purpose was in the context of a child.

The minister came before us a few weeks ago. He said, “I have this bill. It's going to do so much work to protect children, but we have to amend it.” Then we had to put a motion forward to get a copy of those amendments. We're here today. I am not going to relent on this until we have more clarification and I hear from as many witnesses as possible to ensure that children's rights are protected.

My question is open-ended. I'll start with you, Mr. Geist. What clauses of the bill do you believe need to be amended to ensure that a child's fundamental right to privacy and their online actions are not used in a way that will compromise them as adults, or at a future period of time in their life?

Dr. Michael Geist: I'll give you a brief answer, but Professor Krishnamurthy, who is one of the witnesses, has done studies and reports on this, so he's probably best suited to answer some of those particular questions. However, I will say two things in response to your opening comments.

First, to reiterate, I think there's general disappointment for many in the lack of prioritization of privacy over the last number of years. Bills, as you mentioned, get introduced and then seem to languish.

I'm glad that we're here now, but I'm inclined to agree with you that the best way to ensure that you get the best time out of witnesses and the best kind of study is to reflect on legislation as it's intended by the government. If we're left with this amalgam of a bill plus comments about where things are headed, that doesn't provide the best sort of study.

In terms of minors, specifically, I'll note that one of the real concerns arises in differing definitions of minors from province to province and the like. Therefore, one thing I think we need to include within the legislation—I know other witnesses have highlighted it—is the need for some sort of consistent definition here so that we know there is that consistency of protection.

Mr. Brad Vis: Thank you so much.

My colleagues tell me that I should be asking this question of Mr. Krishnamurthy. I apologize. I missed the opening statements. I was debating Bill C-34 in the House of Commons.

Would you like to comment, sir?

Mr. Vivek Krishnamurthy: Thank you very much.

I agree with Professor Geist's initial responses, but let me just take a step back.

There are certainly specific clauses of the bill that could be amended to improve the protection of children and minors. However, we need to consider the structure of the bill as a whole in protecting children—and adults, for that matter.

Several witnesses—not only Professor Scassa and Professor Bennett—spoke about the interaction between the legitimate interest exception and the implied consent provisions of this bill. When they are applied to minors, structurally speaking, those exceptions could be very problematic. I think we need a structural approach to this. All of these pieces of this bill interact together.

What are the exceptions to consent? What are the situations in which someone collecting or using data has to go through a process to justify that? That's a data protection impact assessment. What are the remedies?

Specifically, there are a few things I would like to highlight, which I think are easy amendments, relatively speaking. The first is the “best interest of the child” language, and that could be inserted into—

● (1650)

Mr. Brad Vis: Excuse me. Was that the language put forward by Mr. Therrien, the former privacy commissioner, in the last meeting?

Mr. Vivek Krishnamurthy: That is correct.

Mr. Brad Vis: Thank you.

Mr. Vivek Krishnamurthy: I think that is a very good first amendment that could be made.

Mr. Brad Vis: Why do you think we need that amendment, specifically? Elaborate on that, please. This is a really crucial point.

Mr. Vivek Krishnamurthy: I think the amendment is important because it will influence the interpretation of all subsequent provisions of the bill.

Including language that says the best interests of the child need to be taken into consideration throughout the interpretation of the subsequent provisions means that if you're doing a legitimate interest analysis, that's going to impact that analysis by the company or other organization that's collecting and processing children's data.

That's a very good thing, and it's in line with what's happening internationally. This is a provision that we see in the U.K. It's in the California legislation. I expect to see this internationally in other jurisdictions as well.

Mr. Brad Vis: Thank you so much, sir.

We're going to work to ensure that the best interests of children are included in this legislation.

Mr. Vivek Krishnamurthy: Thank you.

The Chair: Thank you, Mr. Vis.

I'll now turn over the floor to Mr. Van Bynen.

MP Van Bynen, I believe we have an issue with your audio. Is your boom properly placed?

Mr. Tony Van Bynen (Newmarket—Aurora, Lib.): Is this better, Mr. Chair?

The Chair: Yes. That is much better.

Mr. Tony Van Bynen: Thank you. I'm sorry. It wouldn't be the first time we've needed to lower the boom in this environment.

In any event, the information has been very informative, and I very much understand and appreciate the concern for consent and privacy.

One of the things I heard earlier was the risk of reticence. If we become too strident in the way we manage data, are we going to be losing innovative opportunities? Are we going to be losing legitimate business opportunities? How can that be structured so that we can balance the interests of both?

I'll start with Mr. Krishnamurthy.

Mr. Vivek Krishnamurthy: I don't think we should view this as a competition between innovation and privacy. The two can be harmonized. The question is, how do we get responsible innovation that respects what I believe is the fundamental human right to privacy that all of us enjoy?

I think it is very instructive to look at what has happened in the European Union since the enactment of the GDPR, which has consent as one of six bases that an organization that collects, processes and uses personal data can use. Legitimate interest is a key part of the European data protection framework, and it is relied upon very extensively to provide all kinds of innovative services. In fact, in the European Union, as far as I know—and this is getting into AIDA territory—it's the main way that training data for AI is acquired.

The European law, unlike what we are thinking of here, includes many more protections around the use of those exceptions to consent. When we are relying on those exceptions in order to get business activity or other forms of innovation, I think it's very important that there are, for example—and I've mentioned this before—data protection impact assessments, to think very carefully and evaluate very carefully the interests of the data processor and what they are doing versus the interests of the people whose data is being processed.

Especially when it comes to data that is sensitive, those protections are extremely strong in the European approach, and this goes to Professor Bennett's point in response to another honourable member's question about interoperability versus harmonization. We can make our law interoperable with other laws, but maybe here is an area where a bit of harmonization with Europe would be good, to protect the privacy rights of Canadians but also to allow us to do business on a transatlantic basis, because we are going to have that strong level of protection that one of our leading trading partners has as well.

● (1655)

Mr. Tony Van Bynen: How would we strengthen the protection of the international transfer of data?

Mr. Vivek Krishnamurthy: I believe this is a question that may be best addressed to Professor Bennett, who has thought about this more than I have.

Mr. Tony Van Bynen: Go ahead, Professor Bennett.

Prof. Colin Bennett: Historically, there are two ways you can do this. You can do it the way that is included in PIPEDA, which is to put the onus on the organization to ensure that, when data is transferred anywhere to a service provider, whether that is in Canada or elsewhere, the same legal protections apply. The problem with that approach is that it relies on contract or other business-to-business agreements, and the individual tends to be excluded from that arrangement.

The other approach is to do what the Europeans have done over the years, which is a legal test, a jurisdiction-to-jurisdiction approach, which is to say, “These are the countries around the world to which personal data might be safely transferred.” The disadvantage with that is that it's a lengthy approach. It's highly legalistic. At the end of the day, it doesn't do a lot to ensure that the data is protected on the ground.

The short answer to your question is that it's complex. As I said, I think the approach that says that when a business is transferring data to a service provider, whether that's in Canada or offshore, it has to do an assessment, not only an assessment of what the company is doing but also an assessment of the legal and political environment.... For economic reasons, our businesses transfer personal data on Canadians to countries around the world that do not have proper privacy protection and, in some cases, have questionable human rights records. I think Canadians would be pretty annoyed about that if they knew it was happening.

A business should have to assess that. This is essentially what the Quebec law says. Do a privacy impact assessment—actually, broader than a privacy impact assessment—and be ready to demonstrate accountability for that data if and when a regulator comes calling.

That would be the compromise approach that I would suggest, but, at the moment, a business looks at this bill and says, “I want to transfer that data overseas. I want that data to be processed overseas. What do I have to do?” It's not clear. There's nothing there. Most legislation, as I said, has a section on international data transfers, and I think that would be something I would strongly advise.

Mr. Tony Van Bynen: With respect to the speed at which this is being addressed, I've often heard that perfection is the enemy of progress. The reality is that the genie is out of the bottle with respect to data processing and with respect to the Internet, and the swift emergence of AI is a matter of concern.

I've heard a lot of things about what is not right in this bill. Can you tell me three things in the bill that we absolutely need to safeguard to make sure that it's effective and that it accomplishes the intent of protecting the privacy of data?

Prof. Colin Bennett: On the powers of the commissioner, there are several things in the bill about the new powers of the commissioner, the penalties and the sanctions, etc., that I think are improvements and for which advocates have been calling for a long time.

The current situation in PIPEDA, where the Privacy Commissioner really just has recommendation powers, has been untenable. Many of us have been saying this for a very long time. Michael Geist testified back in the day and so did I. To give the Privacy Commissioner more teeth, more bite, is a clear improvement, not only in terms of fines and administrative penalties, but also some of the other things in the bill that he is able to do.

I'd just leave it at that and perhaps my colleagues could also add.

● (1700)

Mr. Tony Van Bynen: Ms. McPhail—

The Chair: I'm afraid we're out of time, Mr. Van Bynen, so we'll have to stop there.

[*Translation*]

Mr. Lemire now has the floor.

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

Dr. Geist, I'd like us to discuss the data the government collects.

Is this something we should be concerned about? Do people feel that the public and private sectors are equally subject to the provisions of Bill C-27? Should we feel reassured? Is our data adequately protected, given what the various levels of government do with it?

[*English*]

Dr. Michael Geist: A conventional way to look at the government-related collection of data is through the Privacy Act lens, which successive commissioners, going back well before even the creation of PIPEDA, have argued is insufficient and inadequate. Government has consistently failed to hold itself to the same standard that it expects of the Privacy Commissioner. We know the reason why privacy commissioners have regularly raised it, but it has rarely risen to the level of actual reform.

If the question is more around political parties and their potential application—we've had several witnesses raise this—I think if we're honest about it, it's pretty obvious why they're not included. It's because political parties have grown addicted to access to that data. They value that data and, quite frankly, they fear that if they had to actually get the same level of consent that they are expecting businesses to obtain from users, they wouldn't get that consent and it would put that data at risk.

For me, this highlights two things. First, I just think it's so obvious: If you claim that there's a fundamental right to privacy and you're going to elevate the expectations for businesses, please put up the mirror and have that same expectation for yourselves as political parties.

It also highlights why there are real challenges with the law with respect to the private sector. Just as political parties don't want to have any sort of limitations on the collection and use of the data outside of some bare bones sort of legislation, so too for lots of businesses. They would also say that they are super innovative and acting in the public interest or have a legitimate interest. We know all the kinds of language that comes out of this. Fundamentally, they don't want to have to ask for actual, informed consent because they know they might not get it.

We can see why you need to ensure in these rules that we hold those businesses to a higher standard. I'd argue that we ought to be doing the same thing for political parties.

[*Translation*]

Mr. Sébastien Lemire: Thank you very much.

The Chair: Thank you.

Mr. Masse, you have the floor.

[*English*]

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

Yes, it's a critical aspect. We didn't do that on the do-not-call list. I think that's a serious void that needs to be looked at, so I appreciate those words.

I know you have hesitations on how we got here, but if you were looking at this bill from our perspective, in terms of trying to make it work, what are the key components that you would suggest right now? I'm sorry I missed your opening elements, but maybe you can build on some of that. What do we really need to do at a bare minimum to get it done?

Dr. Michael Geist: I guess I will start.

Part of the problem that I see—and I think it's been echoed by some of the other witnesses, who may want to chime in—is that this omnibus approach that has combined both privacy and AI fundamentally really impairs the ability to have an effective review of the legislation as a whole. We are unsurprisingly having much of our discussion on the privacy side, which I understand. That's where the committee was driving, at least initially, but the AI rules are critically important. As we've said, we don't even have the full text associated with them, and the implications are enormous.

To me, the starting point fix for this committee is to say that this is not working the way it needs to work for the committee to do its job effectively. You want to shelve the AI portion altogether for the moment and either go back to the drawing board or say that you're going to conduct two studies or that two committees are going to conduct studies. Perhaps ETHI gets involved. There has to be some sort of mechanism where both of these different pieces of legislation get the kind of attention they deserve.

In terms of the privacy side, very quickly, on this bill, I've highlighted the political party side. I guess I would again emphasize that we will hear, and we do hear, from many of our witnesses that we need to be innovative. We can't be out of step with these things. I have to say that you need to recognize that this is going back to the hearings in the 1990s. We saw the same kind of idea that the sky is falling if you legislate in this way. You saw the same kind of comments being made in Europe when the GDPR was being developed. The reality is that businesses will adapt. They will adopt those rules and, in many instances, find competitive advantage for doing so.

I would urge you, as you go through the bill, to look for where can it be strengthened and where there are some exceptions—we heard today about many of the exceptions that are problematic—but, most fundamentally, recognize that the lens that needs to be brought here is not one of the scare tactics of "You're going to harm innovation in this country", because that's just the basic playbook on privacy rules. It's rather how we can ensure that we have the best possible law looking a decade or two decades ahead.

● (1705)

Mr. Brian Masse: Just on a quick point, Mr. Chair, that's why the NDP asked the Speaker for a ruling about this bill. It's split in terms of votes in the House on the two components, the AI and the other one, because they really were inappropriate. We're going to study them together here, but the voting in the House of Commons will be separated into those two elements.

Thank you, Mr. Chair.

The Chair: Thank you, Mr. Masse.

Mr. Perkins, you have the floor.

Mr. Rick Perkins: Thank you, Mr. Chair.

I'm sorry. I had an urgent call. I had to leave, so like MP Masse, I apologize if somebody covered this.

My first questions will be for Dr. McPhail.

I want to start by saying that we've had some interesting testimony already, and some pulling of teeth out of the minister to get the amendments he said he would make and then refused to make and then did make as drafts—which I think, in some cases on privacy, are wholly inadequate.

You know, we had Bill C-11, which the Liberal government brought in and which was flawed. They didn't listen to the privacy commissioner of the day and got responses afterwards, when it was tabled, that it was a bad bill. Then the 2021 election came along, so it died. The minister didn't listen to the testimony and brought in a flawed bill again, and let it sit in the House for a year before we debated it. Then, at the last minute, after four years of battling back and forth, he decides that maybe individual privacy matters, so we'll recognize a fundamental right.

Here's my problem with where the government is, and I think Dr. McPhail and Dr. Scassa outlined some of the reasons. If you had watched my earlier questioning.... While the Liberals are going to put the fundamental right in the "Purpose" section, the most important section, they also say the ability of an organization to use that data is basically of parallel importance in the purpose of the bill.

Then, as you've pointed out, there are issues in proposed section 12 around consent and implied consent. Quite frankly, I thought implied consent was gone a long time ago, in the 1990s, like reverse consent. Apparently, implied consent still exists here, so I can just say, "No problem, Brad. I think you would have consented to this, so I'll use it anyway."

Then, in proposed subsection 15(5), as pointed out in the testimony we had earlier, there's a huge problem.

Proposed section 18, which I've talked a lot about, basically says, "No problem. Big business can use your data, no matter what the consent is, if it's in their interest to use it, even if it causes harm."

Then there's proposed section 35. I brought up proposed section 35 to the former privacy commissioner last time. It says that if an organization is using your data for research or statistics, it can use the data however it wants—unidentified, directly. It doesn't say, like PIPEDA used to say, that it is for scholarly work. Those words are no longer there. It says that an organization can use it, and “an organization”, as we know, in this bill is a business.

There's a lot to fix in this bill to put the balance back on the individual. The Liberals have put the balance on big, multinational data-mining companies—Facebook, Google and others—to have the rights to do whatever they want with an individual's data. I am wondering, is it simply removing proposed section 18, the legitimate interest, that puts the balance, or do you have to make another statement of a higher level in the “Purpose" section? Do you have to get rid of proposed section 35 and replace it with what already existed in PIPEDA that's being removed here?

Maybe I could ask Dr. McPhail and then Dr. Scassa to comment.

● (1710)

Dr. Brenda McPhail: The simple answer is this: It's not simply proposed section 18; there are a series of interlocking flaws with the bill. One of the other witnesses mentioned that you have to look at this bill in a totality. The clauses work together, so there are, as you have stated, many places where amendments could be used to strengthen the bill.

Adding the fundamental right to privacy is an important one. I would reiterate my comment that it really needs to be embedded more substantively within the bill, precisely for the reason you've identified. One of the ostensible purposes of the bill is to balance what is now an individual's right to privacy with a business's interest in collecting and using information. To make sure we get that balance right, we need to make sure that the weighting of an individual's right is proportionate to the way we're looking at the business's interest. Adding that fundamental language is important, and there are a number of places—which I'd be happy to document in writing later—where I think the bill could be improved by adding it.

Mr. Rick Perkins: Thank you.

Dr. Scassa, go ahead.

Dr. Teresa Scassa: One of the real challenges with this bill is that it's not just specific, targeted amendments to the law that we had in place before, but it's a complete rewriting and reworking. Many of these provisions have come over verbatim from PIPEDA, but related concepts have been changed or redefined. In some cases, there have been new provisions added and new language used. As a result, there's a lot going on and there are substantive concerns, and then there are the concerns about how the provisions interact with each other. There are concerns about whether there are legacy problems created because things have been carried over but not adapted to other concepts that have been introduced in the bill.

I think all of us who have been studying and looking at this bill, when we were asked to name the top three things, came up with lists of 15 or 20 or 25 things and thought of those as short lists, because there's a lot that you could comment on and address. I think we've been trying to move up to the top things.

I'm very concerned that if this bill is passed, over the course of the next few years we're going to be finding problems and issues in the bill relating to some of these other changes and language adjustments that we didn't address or didn't anticipate. I think this is a concern, particularly in light of Professor Geist's comments that it takes an awfully long time before there's room on the legislative agenda for further amendments.

I think this is one of the fundamental challenges of this bill. I am sorry that this committee cannot fully devote its time to this and has to split the time between this and the AI and data act, which is very seriously problematic as well.

Mr. Rick Perkins: I'd like to quickly ask Mr. Geist about Dr. Scassa's comment about proposed section 51 and the ability to scrape data and use that publicly available information. I wonder if you would comment on that danger that this bill opens up.

Dr. Michael Geist: I think Professor Scassa is exactly right. Anyone who's been paying any sort of attention over the last five to 10 years recognizes that in what we once thought of as data that is open and may be used, oftentimes we're talking about data that didn't have the appropriate consent in the first place, and certainly not necessarily the consent for the kinds of reuse that you start to see online. Simply couching it as, “It's available, so you can use it”, without recognizing that many of those uses may be wholly different, even if there was consent obtained.... Sometimes there may not have been, but even if there was consent, it may not be related to these new kinds of uses, so we have to tread really carefully.

The Chair: Thank you very much.

I'm afraid that's all the time we have, so we'll turn now to MP Lapointe for five minutes.

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

My question is for Mr. Krishnamurthy.

You wrote an article in May 2022 called “With Great (Computing) Power Comes Great (Human Rights) Responsibility: Cloud Computing and Human Rights”—great title, I might add. In the article, you stated that the human rights impacts of cloud computing have not been studied to nearly the same extent as newer technologies that are powered by the cloud. Can you expand on this in relation to Bill C-27, recognizing privacy as a human right?

● (1715)

Mr. Vivek Krishnamurthy: Thank you for that question, and also for reading my scholarship, which I appreciate. It's nice to see that it does get read.

I'd actually like to address that question, if I can, in connection with the previous discussion around proposed section 51 of the legislation, which is about how data can get reused with publicly available information, or earlier in the statute with regard to statistical and other kinds of purposes. I think this is a key point of interaction between the CPPA and AIDA—if you want to be operatic about it.

Technology is changing very quickly, and we are seeing a proliferation of extremely powerful technologies—we'll call them AI—that have an interesting business model. The business model is that smaller and smaller companies—those with less capacity than previously in terms of compliance, regulatory affairs and legal—are able to leverage extraordinarily powerful tools and do incredible things with our data.

In the article, I talk about a company that just takes pieces of Amazon's cloud offerings—a voice recognition system, a translation system or a transcription system, data analysis—and creates automatic systems to monitor prisoner phone calls. The uses to which personal data can be put once collected, because of the AI environment we live in and the fact that these technologies are available with the swipe of a credit card to anyone, regally change what we are talking about when we talk about privacy.

PIPEDA was enacted 25 years ago. We could not have foreseen this revolutionary change, and now we have this legislation and its two central components. Of course, there is the procedural one with parts that would establish the tribunal. Given that changing landscape, and given what we think is going to happen in the next 15, 20 or 25 years with regard to technological advances that can more efficiently use our data and determine things about us that we didn't know, we need to be extremely thoughtful about both parts of the legislative package.

Again, I believe Dr. McPhail mentioned this. The CPPA is the statute that governs the input of data into AI systems, for better or for worse, and the AIDA will hopefully, with amendment, regulate the uses to which the systems can be put. I think it is a critically important intersection that this committee needs to think about very carefully as technology becomes more powerful and accessible to more and more actors.

Ms. Viviane Lapointe: That's a really interesting position on that.

Do you have real-world examples that you can share with this committee to demonstrate the instances of human rights and privacy challenges?

Mr. Vivek Krishnamurthy: I think an excellent example that should be on this committee's mind and those of all Canadians is Clearview AI, which is a technology company based in the United States that takes publicly available information—your photos on Facebook, on Tumblr or whatever else—and has developed a very powerful AI-based facial recognition system, using publicly available information, with no consent for the collection or use of that. Of course, all the privacy commissioners who studied this came to the conclusion that this violates basically all existing Canadian privacy laws.

In this case, we have a company that is based in the U.S., so there are questions about how applicable the law is, but I think it demonstrates several things. It demonstrates how some of these exceptions are very susceptible to powerful forms of misuse, and then once you have ingested the data and trained the model, we also need the regulation of how it's used.

One could argue that there are some purposes where publicly accessible information can and should be collected and used. We can talk about that. However, the fact that it's not subject to any oversight—an impact assessment requirement, for example—is problematic when it comes to the CPPA part of the bill, and then we can talk separately about the many weaknesses of AIDA.

Ms. Viviane Lapointe: Do you have any practical suggestions for this committee on how the legislation can address these human rights concerns?

● (1720)

Mr. Vivek Krishnamurthy: Many of my colleagues who conceptualize privacy legislation think about its substantive provisions—you can do this and you can do that—and also about privacy law as a process. The idea is to get organizations that collect and use personal data to build governance and accountability around how they do so. It's thinking very carefully about what the uses are, documenting that and having checks.

In my earlier comment, I talked about the overall framework of the legislation and the interacting components. This is where I believe a stronger process orientation in both.... In the CPPA, that's the data protection impact assessment provision, which will interact subsequently with enforcement provisions. When it comes to AIDA, it's making clear some uses that are beyond the pale, which we're going to forbid, and then calibrating the legislation to the level of risk. Right now, AIDA really only governs systems that are high-risk and we don't know what those are because the criteria are not there.

The European law, which I think is weak and could be improved, governs all AI systems presumptively. Even those that are low-risk, where the people who are developing those systems have actually shown that the risk is low, are subject to requirements. I think that's a key safeguard. If we're going to create legislation that is going to be durable for a long time, it needs to assess that entire risk environment and capture it in the legislative package.

The Chair: Thank you very much.

I'll now turn to Mr. Williams.

Mr. Ryan Williams: Thank you, Mr. Chair.

Mr. Geist, tell me a little bit about the high-impact systems using search and social media and compare that to algorithms for search results. How does this bill address that? What changes would you make?

Dr. Michael Geist: Thanks for the question.

Technically speaking, the bill doesn't address it because we have the bill. What we also have now, as you know, is essentially a memo from the minister that highlights that they've begun to identify what they intend to include within the high-impact systems. As we just heard from Professor Krishnamurthy, the approach is to seek to regulate those and establish a number of regulatory frameworks around those provisions.

There is generally a consensus that it's appropriate and necessary to have rule sets, particularly where there are concerns around bias coming out of AI systems. Think of the use of AI in labour markets for hiring. Think about it in the health sector, in the financial sector and in law enforcement. There are a lot of places where we can easily identify potential risks, potential harms and the like. That's where much of the discussion has been.

Oddly, at least in terms of the list that has been provided, search engine algorithms and social media algorithms are included here as well. Unquestionably, we need algorithmic transparency with respect to these companies. We need to identify ways to deal with the potential for harms that are coming out of this, such as any competitive behaviour in search results, which is clearly an issue that is raising some significant concerns. However, I find very puzzling the notion that we would be treating that as a high-impact system in the same way we would treat law enforcement's use of this or health uses. I'm not aware that anyone else anywhere in the world has seen fit to do that as they work through some of these questions.

Mr. Ryan Williams: Thank you.

I'll cede the rest of my time to Mr. Généreux, Mr. Chair.

[*Translation*]

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

I would like to thank my colleague for sharing his time with me.

I'd like to thank all the witnesses for being here.

Dr. Geist, I'd like to talk about the way this bill, formerly Bill C-11, has been presented over the past two years. We know that amendments were requested and that the minister didn't really listen, because the new version is no better. So here we are, 18 months later, and you are having to testify about this bill.

During this whole process, which is set to last several months, we will be meeting with about 100 witnesses. How do you feel about this process, when we haven't had access to the eight amendments put forward by the minister, other than the few lines we've be able to get so far? I'm asking because you talked about this earlier.

I'd like you to speak as a witness. I'm not necessarily asking you to speak on behalf of others, but at the very least I'd like people to understand the process we are currently in, which I consider to be skewed. How can you or any of the witnesses who will appear possibly give your opinions on the content of a bill without access to the amendments?

● (1725)

[*English*]

Dr. Michael Geist: First, I'll say that there were improvements made from the prior bill to this bill, so the government did listen, and some of the things that are in this bill are better than the one that was introduced in the first instance and really didn't go anywhere.

I will also say candidly that I must admit that this is one of the hardest committee appearances that I've had in a very long time, in part because typically, when you're invited—and I have appeared on omnibus legislation before like the one we get with, let's say, the budget implementation act—you're invited for a specific kind of provision, and we recognize how that works.

In this instance, we really have two distinct bills, perhaps more than two, but two fundamentally on those two issues, plus, of course, the tribunal. You get five minutes. I recognize that you don't get multiple appearances, and you don't get multiple amounts of time to deal with it. I do think, as I look around, that the witnesses—people like Brenda McPhail, Professor Krishnamurthy, my colleague Teresa Scassa and Professor Bennett—have enormous expertise across the board. There is some correlation here.

This strikes me as not just an inefficient way of dealing with this, but I think, if I'm honest about it, that it's an ineffective way of trying to be effective with the responses that I'm giving. There is obviously a limit from a time perspective, a limit in terms of what I could prioritize and the kinds of issues that I try to highlight. Something's got to give, so to speak. At the end of the day, you can't talk about everything, and this would have been far better, I think, had we divided the two.

[*Translation*]

Mr. Bernard Généreux: I have another question for you.

Earlier, you said that the legal provisions were always more in favour of businesses than individuals. You talked about balancing the playing field.

What exactly did you mean by that?

[*English*]

Dr. Michael Geist: That was a reference, and we've heard it regularly, to a desire to strike a balance within these provisions, but let's recognize that, once you get outside and start applying these rules, it's not a balanced playing field. Many individual Canadians don't know their privacy rights or, if they do, the prospect of filing a complaint, proceeding with it and facing all the challenges that are inherent in the system—and this is true for more than just privacy, but it's certainly true with privacy—is enormous.

We've had a system that, for the last two decades, has left people really disappointed because oftentimes they go through that process and are left with nothing other than a non-binding finding.

I'm glad that this law seeks to remedy that. The enforcement side is important, but we need to realize that, especially as we bring in tougher penalties, which are one of the really good things that I think are in this legislation, it also means that those who are facing the potential for penalties are going to take a much more aggressive approach in terms of how they deal with these various complaints.

It's not a level playing field, which means that you need to embed as much as you can within the legislation to limit the ability of those businesses to take advantage of what is quite clearly a power imbalance between themselves and the individuals.

[*Translation*]

The Chair: Thank you very much.

Mr. Turnbull, you have the floor.

[*English*]

Mr. Ryan Turnbull (Whitby, Lib.): Thanks to all the witnesses. I'm sorry I missed a portion of it. I was in the House speaking to another piece of legislation, but it's great to have you all here, and your expertise is greatly appreciated.

Mr. Geist, you said moments ago that improvements have been made. You've been somewhat critical today, I have to say. I wonder if I could ask you to acknowledge some of the improvements that have been made and maybe give a little bit more detail about those so we can acknowledge that as well.

Dr. Michael Geist: Sure. I want to speak specifically to highlight the importance of this legislation and how important it is to include far-improved enforcement measures. I think the experience over the last couple of decades is that for many.... If all you're left with are non-binding findings, it is very tough to enforce, and it is, I think, tough for the commissioner to ensure that companies themselves are compliant, because they will naturally engage in a bit of a risk analysis, at least under the current bill. They'll ask, "What happens if I don't comply?" or "What happens if I push the envelope a little bit?" The answer is that you might face an investigation if someone realizes and files a complaint, and, at worst, at least initially, all you're going to get is a non-binding finding, and you need to try to do something. We've even seen that. I can recall an incident, I believe it was with Bell, which rejected some of the initial findings of the commissioner, so there was some pressure, and they came back.

We've seen companies take a pretty aggressive approach. I'm glad that the government has seen fit to really improve on the enforcement side, both in terms of the powers the commissioner has and in terms of the penalties that are associated with the legislation. I'm glad it's seen fit to begin to adopt some of the kinds of provisions that we've seen in Europe. It's long overdue, and they're not quite the same or at least identical, but, nevertheless, it moves us in a direction.

Absolutely, I think there are things that improve on our existing legislation. That legislation is more than 20 years old. We need to fix the legislation, but, as I said, the point of emphasis for me, and we've heard it from others as well, is that if you're, in all likelihood, fixing this bill or this legislation only every 10 or 20 years, you can't rest on your laurels and say, "Here, we got a bunch of things right", when there are all sorts of other things that need fixing.

● (1730)

Mr. Ryan Turnbull: Would you agree, then, that it's really important to see this bill through, given the fact that our legislation is 20 years old, recognizing for sure that we have to have a critical lens as we debate this bill and certainly work toward strengthening it? I know you've outlined multiple ways, but what are the repercussions if this bills fails? It has once before, so I think we need to really push forward. Could you speak to that? How are Canadians going to be impacted if we don't have updated legislation?

Dr. Michael Geist: I'll speak candidly and tell you that with the first bill, with all due respect, the government did not move forward with it in any meaningful way at all under Minister Bains. That's just the reality. With this bill—and I can't speak for other people coming out of the privacy community—I feel it is a source of significant frustration that we get a bill that barely makes it through anything. This one also took a year from introduction until we're finally before committee. We have two bills or three bills embedded within the same legislation, and then the question is posed, "It might not be ideal, but isn't something better than nothing?"

Yes, something is better than nothing, but if we are truly going to try to prioritize privacy as such a critical component, I believe Canadians expect better than a bill that doesn't really meet the kinds of expectations that have been regularly identified before you.

Mr. Ryan Turnbull: Maybe I can ask you, Mr. Krishnamurthy, whether you feel the same way or whether you can recognize there are some significant improvements in this bill. What would be the repercussions if we don't move forward with updated legislation?

Mr. Vivek Krishnamurthy: Undoubtedly, the Bill C-27 package of amendments is an improvement over the status quo. I think all of us would acknowledge that. However, I'm not sure we should settle for a C+ bill. I think Canadians deserve A+ privacy protection, and amendments to this bill can get us there.

I think that is the spirit in which all of us who are scholars and activists, and who think about privacy and take a big-picture approach to this, think of it. We understand that private information does need to be collected and processed, but that needs to be done in a way that respects what is a very fundamental human right, one that is becoming more important in our digital age over time, as technology becomes more invasive, and it is important to get that right.

Political oxygen is scarce. Again, you have many priorities, many things to legislate, so if this is our shot, we have to do our very best. I think everyone here today has provided lots of really good ideas, and if this committee would embrace them and enact some amendments, this could be a much better bill.

Mr. Ryan Turnbull: You're speaking to the importance of this process, which I think we're all very committed to. I was just trying to get a sense of what the repercussions are going to be if this bill stalls any longer, but I think you've answered that well enough.

Maybe I'll just say quickly a couple of things based on some testimony we've heard.

The AIDA portion of this bill went through over 300 consultations, so I think there has been a lot of consultation that has happened. I'll just put that out there.

In relation to some of the comments made about political parties, the government has been carefully studying the Chief Electoral Officer's recommendation on strengthening privacy measures. We will have more to say about that in due course. Just to let you know, just for information purposes, I think that's helpful to reassure folks.

Maybe I'll leave it there.

The Chair: Thank you, MP Turnbull.

[*Translation*]

Mr. Lemire, you have the floor.

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

We've had some meaningful discussions. However, I'm wondering whether this committee will really have the will or capacity to move quickly and help get this bill passed. To be honest, I even wonder if the government really wants to get Bill C-27 passed at this point, in the context of this legislature.

Having said that, I feel like asking you some questions, Dr. McPhail.

In your publications, you put a great deal of emphasis on developing responsible artificial intelligence and transparent governance of artificial intelligence.

Because the rapid development of technology poses significant data security and privacy challenges, what are your thoughts on establishing a technological sandbox that would isolate emerging technologies in a separate environment, with a view to assessing their compliance with privacy standards before they are made available to the public?

● (1735)

[*English*]

Dr. Brenda McPhail: Thank you very much for that question.

There are a range of ways in which the AIDA could be improved to facilitate truly responsible AI governance.

The idea of a sandbox is an interesting model. One of the big problems with the ways artificial intelligence tools are currently developed is that they are created and tossed out into the wild, and then we see what happens. A sandbox, to the extent that it would be able to mitigate that kind of risk, is a really interesting concept. I would note that there's absolutely nothing in the current bill that actually fosters the creation of such a sandbox at this time.

Of course, that's only one of the many gaping holes in the truly skeletal structure of AIDA, which, even with some of the potential amendments that have now been floated, still has a long way to go in order to be the effective bill that people across Canada deserve. That is why many of us have actually called for a reset of that bill, rather than a revision. It is so fundamentally flawed that it's hard to imagine how you're going to make it something that truly respects Canadians' rights and truly reassures Canadians that artificial intelligence is a tool that can be used across all sectors of our economy as it is envisioned to be used, safely and with respect for their privacy rights.

We've heard a little bit about reticence risks. I would counter reticence risks, which is a business concept, with social licence. Members of the public are deeply concerned that their information is being collected and used in ways that they don't understand, often without their consent—something the CPPA would facilitate—and for purposes that they disagree with fundamentally.

If we allow our AI act to take that data, collect it in that way, and leverage it in tools that, again, members of the public find difficult to trust, we are not fostering a vibrant innovation economy in Canada; we are fostering a distrustful society that will not believe their government has their back, and we will be genuinely reticent as citizens to use these technologies in a way that we would like to, if we take seriously the idea that this technology has immense potential to improve our world, used responsibly.

[*Translation*]

Mr. Sébastien Lemire: Thank you very much.

My time is up.

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

[*English*]

I have no more speakers, so I'll yield the floor to myself.

My first question is regarding proposed section 35, which MP Perkins brought up. I'll ask Professor Geist, but if anyone wants to volunteer comments.... Proposed section 35 provides that “An organization may disclose an individual's personal information without their knowledge or consent”. Proposed paragraph 35(c) is, to me, the oversight of that disposition, which requires the organization to inform the commissioner of the disclosure before the information is disclosed.

Is this a sufficient form of oversight for that sort of transmission of personal information?

Dr. Michael Geist: I think there's reason for concern based on the load that the commissioner is facing, realistically. We've had a situation for the last number of years with the Privacy Commissioner where findings sometimes run between 12 and 18 months because there simply haven't been the resources to deal with issues.

If this gets interpreted aggressively by organizations to say, "Well, it's impractical to obtain consent, so let's just run off and ask the commissioner", I think there's a concern that there will be delays, which businesses aren't going to be happy with, but there's also the question of whether this is going to get the sort of study that's necessary.

I'd be curious to hear what some of my colleagues on the panel think.

● (1740)

[*Translation*]

The Chair: Thank you.

[*English*]

Professor Krishnamurthy, go ahead.

Mr. Vivek Krishnamurthy: I think it's positive that the disclosure does need to be made to the commissioner when this happens. However, I think we need to question how much oversight the commissioner can exercise.

Again, this is a point where an interaction between the CPPA and AIDA.... What kinds of research for statistical purposes might organizations make? It might well be to train AI models. We now know from research that when data is used to train an AI, AI systems can retain that data. I believe the technical name is "imprinting". If you use ChatGPT and you use it hard, you can probably get an AI system to spit that data back, and that's a big problem.

The mere disclosure to the commissioner that this is happening, without some kind of analysis of what the risks are.... This is why I keep coming back to this data protection impact assessment point. It's so important that this weighing occurs. What are the relevant risks?

We want to incentivize research, of course, but let's remember that Cambridge Analytica was a research organization. It was a research disclosure of data that was the beginning of that terrible privacy scandal. That safeguard alone is not enough. I think we need more.

I'm very interested in research. I'm at an academic institution. I want to promote that. It's a very pro-social thing, and there is a real anti-commons problem with trying to get individual consent every time, but the safeguards need to be stronger.

The Chair: The second question is regarding proposed section 39, "Socially beneficial purposes". My understanding is that the information needs to be de-identified and it can be shared with the government or government institutions, with health care institutions or post-secondary educational institutions. I gather it would be, for instance, at the request of a government department or organization that the information, which is de-identified for sure, is shared.

I'm just wondering if there should be the same kind of oversight here that we see in proposed section 35, where at least an organization that is transmitting this information to the government is required to disclose that. Otherwise, we can envision ways in which that would happen where the public wouldn't even be aware that this information.... I get that it's for socially beneficial purposes, but that can be interpreted quite broadly.

Professor Geist, go ahead.

Dr. Michael Geist: Yes, I think that's right.

Professor Scassa has done a lot of study on that and she is probably ideally suited to comment.

I think you answered the question yourself. It does indeed open the door to very broad interpretation, which I think is a source of concern.

The Chair: Professor Scassa, go ahead.

Dr. Teresa Scassa: I completely agree that there are problems with this provision.

The one I flagged in my opening comments is that it refers to de-identified information. This was taken verbatim from Bill C-11 and put into Bill C-27, but in Bill C-11, "de-identified" was given the definition that is commonly given to anonymized information.

Under Bill C-27, we have two different categories: de-identified and anonymized. Anonymized is the more protected. Now you have a provision that allows de-identified information—which is not anonymized, just de-identified—to be shared, so there has actually been a weakening of proposed section 39 in Bill C-27 from Bill C-11, which shouldn't be the case.

In addition to that, there are no guardrails, as you mentioned, for transparency or for other protections where information is shared for socially beneficial purposes. The ETHI committee held hearings about the PHAC use of mobility data, which is an example of this kind of sharing for socially beneficial purposes.

The purposes may be socially beneficial. They may be justifiable and it may be something we want to do, but unless there is a level of transparency and the potential for some oversight, there isn't going to be trust. I think we risk recreating the same sort of situation where people suddenly discover that their information has been shared with a public sector organization for particular purposes that have been deemed by somebody to be socially beneficial and those people don't know. They haven't been given an option to learn more about it, they haven't been able to opt out and the Privacy Commissioner hasn't been notified or given any opportunity to review.

I think we have to be really careful with proposed section 39, partly because I think it's been transplanted without appropriate changes and partly because it doesn't have the guardrails that are required for that provision.

● (1745)

The Chair: Again, feel free to send any suggestions on how we could strengthen proposed section 39. You have mentioned some already with regard to anonymized instead of de-identified, and also if the organization needs to inform the commissioner. If you have any specific wording—and this goes for all witnesses—you can send through the clerk potential amendments you deem worthwhile.

I have one last question.

Are there jurisdictions where a constellation of publicly available data on an individual becomes sensitive information—personal information that ought to be protected? With the systems that are capable of gathering publicly available information, when you gather enough data points on an individual, it can become sensitive.

Are there jurisdictions that do that? Are there examples you can point to?

Dr. Teresa Scassa: One example would be Clearview AI scraping publicly available information. They scrape photographs of individuals from publicly accessible websites. Then they create biometric face prints of those individuals in order to create their facial recognition database. We all accept.... It's broadly understood in the privacy community that biometric data is sensitive information.

A picture of you receiving an award at a public event or giving a speech as a member of Parliament, for example, is turned into biometric data that populates a facial recognition database. I think it goes from being an innocent photograph to sensitive biometric data very quickly. That's just one example.

The Chair: Professor Krishnamurthy, go ahead.

Mr. Vivek Krishnamurthy: Mr. Chair, directly responding to your question, article 9 of the European Union's GDPR is very instructive in this regard, because it says that the processing of personal data that reveals sensitive characteristics is subject to the heightened protections for sensitive data. So, the data may be anodyne at the beginning, but as I tell my privacy law students, what I buy at Loblaws can be very revealing of my health, if I'm buying lots of potato chips and not a lot of fresh fruit. That can become health information through processing and through the correlation of my data on my shopping habits with large-scale statistical studies.

I think that's a very important point that you've raised about protecting what the processing reveals.

The Chair: Thank you very much.

I know, Mr. Perkins, you wanted to ask one last question. Be very brief, please.

Mr. Rick Perkins: Perhaps I could ask Dr. McPhail.

In your opening testimony, you mentioned that we need to dig deeper in AIDA than high-impact systems, which the minister has defined, and now redefined. At what level, then...? Could you expand on that a little more beyond high-impact systems? One, is "high-impact" now properly defined? Two, what other level or examples of things do you think need to be incorporated or captured by the AIDA portion of this bill?

Dr. Brenda McPhail: Thank you for that question.

I think it's been mentioned already today, but I will repeat it. Merely looking at high-impact systems, however they are defined—and right now that's unclear in the current amendments—is not enough to fully mitigate the risks of AI, particularly the collective risks to communities and groups. That kind of risk, furthermore, is not covered under the current definition of "harm" in the bill, which is focused strictly on individuals and quantitative forms of harm. In looking at how you can restructure that better, you could look at the European act, but I would refer you to something closer to home.

The Toronto Police Service recently did an extensive public consultation and developed rules on artificial intelligence for use by their service. They adopted a tiered approach, where there are some systems that are deemed low-risk, but require an assessment in order to determine that they are so. There are some systems that are deemed medium-risk, and there are different sets of precautions and safeguards in order to ensure that those risks are appropriately analyzed and mitigated prior to the technology being used. There are also systems that are considered high-risk, which have the highest level of protections and safeguards. Then there are systems that are considered beyond the pale. Some systems are considered so risky that it is not appropriate to use them in a country governed by the Charter of Rights and Freedoms and where democratic freedoms are valued.

That's a much more tiered and nuanced approach requiring assessments at different stages, and then proportionate safeguards and restrictions, depending on the level of risk, can be much more finely tuned and much more responsive to the genuine concerns that members of the public have about ways that AI systems can be used for them or against them in violation of their beliefs and values.

● (1750)

Mr. Rick Perkins: Could we get the library to provide us with a little outline of the Toronto Police Service policy that was just referred to?

The Chair: I'm sure it can be sought for. It's available online.

Thank you very much.

This concludes our meeting.

Thanks to all our witnesses. It's been a very informative discussion.

Thanks in particular to Professor Bennett. We've seen the day rise in Australia through the blinds behind you. Thanks for waking up so early to meet with us. It's much appreciated.

[*Translation*]

I'd like to thank the analysts, interpreters, clerk and support staff.

The meeting is adjourned.