HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

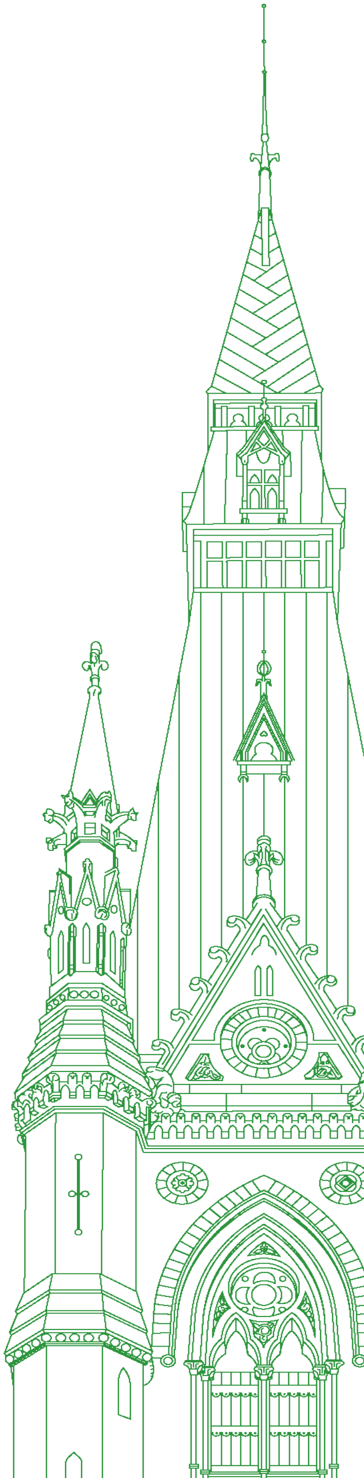
44th PARLIAMENT, 1st SESSION

Standing Committee on Industry and Technology

EVIDENCE

NUMBER 098

Thursday, November 23, 2023



Chair: Mr. Joël Lightbound

Standing Committee on Industry and Technology

Thursday, November 23, 2023

● (1535)

[*Translation*]

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

Good afternoon, everyone.

Welcome to meeting No. 98 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. We have Michael Beauvais, a doctoral candidate at the University of Toronto Faculty of Law, by videoconference; Avi Goldfarb, a professor of marketing and the Rotman chair at the University of Toronto Rotman School of Management; Michelle Gordon, lawyer and founder of GEM Privacy Consulting; Antoine Guilmain, counsel and co-leader of National Cyber Security and Data Protection Practice Group at Gowling WLG; and Luk Arbuckle, chief methodologist and privacy officer at IQVIA Solutions Canada Inc.

Each of you will have five minutes for an opening statement.

Thank you all for taking the time to join us in this study this afternoon. Without further ado, I'll give the floor to Mr. Beauvais for five minutes.

[*English*]

Mr. Michael Beauvais (Doctoral Candidate, Faculty of Law, University of Toronto, As an Individual): Thank you, Chair Lightbound and members of the committee, for today's invitation.

I'm a doctoral candidate at the University of Toronto's faculty of law, and a graduate fellow of the Schwartz Reisman Institute. I have more than a dozen peer-reviewed publications and numerous policy interventions on privacy and data protection law in Canada, the European Union and the United States.

I submitted a brief on children's issues in the consumer privacy protection act with my colleague, Leslie Regan Shade, who is a professor at the University of Toronto's faculty of information, a faculty affiliate of the Schwartz Reisman Institute. I am here today in my personal capacity.

Children's privacy in the digital environment is essential for their agency, dignity and safety. Indeed, data protection laws are one important piece of a response to mounting evidence that corporate surveillance and persuasive design are undermining children's agency and well-being. At the same time, though, digital technologies are vital for children's inclusion and participation in society. Members of the committee, you are in a special position to help ensure that the digital environment aligns with children's rights.

Before highlighting a few of the recommendations made in our submission, let me note that the UN Committee on the Rights of the Child has consistently recommended more robust and standardized mechanisms for meaningfully obtaining children's views on legal and policy matters affecting them. It is thus regrettable that there is no evidence of youth consultation for this important bill. I respectfully urge you to solicit their views.

Let me briefly discuss our recommendations.

First, several key definitions need to be clarified. These include a definition of a minor and a definition of capacity to determine when a minor is “capable” of exercising rights and recourse under the act. The act must also clarify the scope of and the relationship between parental and child decision-making. Additionally, more specification is needed with regard to what happens when minors reach the age of majority. Information about one's childhood should, furthermore, remain “sensitive information” even after one has attained the age of majority.

Second, the best interests of the child should be included as a fundamental principle in the act. Doing so would make the child's interests a primary concern in all aspects of the proposed legislation. For example, the best interests of children should matter in specifying the purposes of data collection, use and disclosure, as well as data retention.

Third, age and parental consent verification requirements and limitations are needed. Treating minors and adults differently makes verification for both age and parental consent an important part of compliance. Such verification, though, can be highly intrusive, unreliable and insecure. Verification also poses serious threats to the freedom of expression of all Internet users.

Fourth, the Office of the Privacy Commissioner should be mandated to develop a children's design code with meaningful participation from youth. Design codes are age-appropriate standards for youth-directed products to ensure the highest level of privacy by design. They also help ensure that youth-directed products do not undermine children's rights. Businesses also welcome the certainty that codes provide. Since codes only elaborate on general principles and obligations arising from the legislation, robust protections for privacy and agency must be in the law itself.

Finally, kindly recognize that providing robust protections for children should not be a justification for meagre protections for adults.

Before concluding, I want to respectfully remind the committee that the ongoing lack of high-speed Internet access among northern, rural, first nations, Inuit and Métis communities deprives children and adults alike in those communities of the same opportunities found elsewhere in Canada. The CPPA's promises and potential are illusory without equitable access to the Internet.

I appreciate your work on this important study, and I look forward to your questions.

Thank you.

● (1540)

[*Translation*]

The Chair: I'll now give the floor to Professor Goldfarb.

[*English*]

Professor Avi Goldfarb (Professor of Marketing and Rotman Chair, Artificial Intelligence and Healthcare, Rotman School of Management, University of Toronto, As an Individual): Thank you for your kind invitation to appear before the committee and discuss Bill C-27.

I'm a professor of marketing at the University of Toronto, where I hold the Rotman chair in artificial intelligence and health care. My research focuses on the economics of information technology, including several papers on privacy regulation and on artificial intelligence.

Canada is a leader in AI research. Many of the core technologies underlying the recent excitement about AI were developed right here at Canadian universities. At the same time, our productivity is lacking. My research has shown that AI and related data-focused tools are particularly promising technologies for accelerating innovation, productivity and economic growth. In my view, a big worry for the Canadian economy going forward is that we do not have enough AI, and so our standard of living, including our ability to fund health care and education, would stagnate. It would be a shame if Canada's research success did not lead to applications that increase Canadian prosperity.

This act is a careful attempt to ensure that Canadians benefit from AI and related data-focused technologies while protecting privacy and reducing the potential for these technologies to harm individuals.

Next, I'll provide specific comments on AI regulation in part 3 and on privacy regulation in part 1. I have specific comments [*Technical difficulty—Editor*] intelligence and data act.

First, the act correctly recognizes that there is always a human or a team of humans behind decisions enabled by AI. In part 1, proposed subsection 5(2) is commendable for noting that “a person is responsible for an artificial intelligence system”. Proposed sections 7 through 9 make these responsibilities clear. In my experience, such clarity about the role of humans in AI systems is both unusual and commendable.

Second, the act constructively defines explainability and transparency in part 1, proposed sections 11 and 12. By making it clear how and why the high-impact system is being used rather than focusing on the inner workings of the algorithm, it will provide useful information without forcing potentially misleading oversimplification of how the algorithms work.

Third, while the details of the act itself implicitly recognize the role of AI in Canadian prosperity, the preamble to the AI and data act does not recognize that technological progress is fundamental to our prosperity, and instead focuses only on regulation and harms.

Fourth, there are two sections of the act that might create incentives not to adopt beneficial AI because the liability is not explicitly benchmarked around some human performance level [*Technical difficulty—Editor*] and safety.

In part 1 of the AI act, proposed subsection 5(1) examines bias. The bias definition suggests that any bias would be prohibited. AI systems will almost surely be imperfect, because they're likely to be trained on imperfect and biased human decisions. Therefore, this definition of biased output incentivizes the continued use of biased human decision-making processes over potentially less biased but auditable AI-supported decisions.

In part 2 of the AI act, proposed paragraph 39(a) examines physical and psychological harm or physical damage. As with bias, the benchmark seems to be perfection. For example, autonomous vehicles will almost surely cause serious physical harm and substantial property damage, because vehicles are dangerous. If the autonomous vehicle system, however, generates much less harm than the current human driving systems, then it would be beneficial to enable its adoption.

The fifth comment on the AI and data act is about the definition of an AI system in proposed section 2 of the AI act: “the use of a genetic algorithm, a neural network, machine learning or other technique in order to generate content or make decisions, recommendations, or predictions.” This definition is overly broad. It includes regression analysis and could even be interpreted to include the calculation of averages. For example, if an employer receives thousands of applications for a job, calculates the average score on some standardized test and uses that score to autonomously select above-average applications to be sent to a human resource worker for further examination, that scoring rule would be an AI system, as I understand it, under the current definition.

I have two specific comments about the consumer privacy protection act.

First, the purpose of the act in proposed section 5 clearly lays out the often competing goals of protecting privacy while facilitating economic activity. While I do understand the wishful thinking that there would be no trade-offs between privacy and innovation, research has consistently documented such trade-offs. Privacy is not free, but it is valuable. Individuals care about their privacy. In protecting privacy, this act will require companies [*Technical difficulty—Editor*] on legal expertise for interpretation. Such expertise is readily available for large, established companies, but onerous for small businesses and start-ups. In the implementation by the commissioner, some direction to reduce any unnecessary burden on small businesses and start-ups would be constructive.

Proposed subsection 15(5) makes the cost of an audit payable by the person audited even if the Privacy Commissioner does not bring a successful case. This creates a large burden on small and new businesses if they get audited unnecessarily.

● (1545)

To conclude, while I have specific suggestions to clarify the language of the act, in my view Bill C-27 is a careful attempt to ensure that Canadians benefit from AI and related data-focused technologies while protecting privacy and reducing the potential of these technologies to harm individuals.

Thank you for this opportunity to discuss my research. I look forward to hearing your questions.

The Chair: Thank you very much.

I'll yield the floor to Madame Gordon.

Ms. Michelle Gordon (Lawyer and Founder, GEM Privacy Consulting, As an Individual): Thank you for the invitation to appear before this committee for its important review of Bill C-27.

I'm a privacy lawyer and consultant based in Toronto. Having worked in the privacy field for over 15 years while raising three sons, I have a passion for children's privacy, and I will focus my remarks on this area today.

My interest in privacy law was sparked when I was a law student down the street at the University of Ottawa, where I did research with Professor Michael Geist and the late Professor Ian Kerr at the time when PIPEDA was a new bill being debated similarly to today's. When Professor Geist appeared here a few weeks ago, he reflected on his first appearance before committee to discuss PIPEDA, noting that it was important to get it right, rather than to get it fast. When Professor Kerr appeared in 2017 to discuss PIPEDA reform, he stated that, at the time, “the dominant metaphor was George Orwell's *1984*, 'Big Brother is Watching You'”, noting that technological developments in the years since PIPEDA go well beyond watching.

Both professors Geist and Kerr were right, especially in the context of children's privacy. Given that children are inundated with emerging technologies well beyond Orwell's *1984*—from AI tools to ed tech, virtual reality and our current reality of watching war and its accompanying hatred unfold on social media—it is more important than ever to get it right when it comes to children's privacy.

When Bill C-11 was introduced in late 2020, it didn't address children at all. As I argued in a Policy Options article in 2021, this was a missed opportunity, given that the amount of online activity for children was at an all-time high during the pandemic.

I commend the legislators for addressing children's privacy in Bill C-27 by stating that “information of minors is considered to be sensitive” and by including language that could provide minors with a more direct route to delete their personal information, otherwise known as the right to be forgotten. I also understand that Minister Champagne proposes further amendments to include stronger protections for minors.

However, as the first witness stated, I think there is more the law can do to get it right for children's privacy. I will focus on two points: first, creating clear definitions, and second, looking to leading jurisdictions for guidance.

First, the law should define the terms “minor” and “sensitive”. Without these definitions, businesses, which already have the upper hand in this law, are left to decide what is sensitive and appropriate for minors. The CPPA should follow the lead of other leading privacy laws. The California Consumer Privacy Act, the U.S. COPPA, the EU's GDPR and Quebec's law 25 all establish a minimum age for consent ranging from 13 to 16.

Further, the law should explicitly define the term “sensitive”. The current wording recognizes that minors' data is sensitive, which means that other provisions in the statute have to interpret the treatment of sensitive information through a contextual analysis, whether it be for safeguarding, consent or retention. Similar to Quebec's law 25, the law should define “sensitive” and provide non-exhaustive examples of sensitive data so that businesses, regulators and courts will have more guidance in applying the legislative framework.

Second, I recommend that you consider revising the law—as an amendment or regulation—in order to align the CPPA with leading jurisdictions, namely the age-appropriate design code legislation in the U.K. and California. Both of these demonstrate a more prescriptive approach to regulating the personal information of children.

The California kids code requires businesses to prioritize the privacy of children by default and in the design of their products. For example, default settings on apps and platforms for users under 18 must be set to the highest privacy level. This is something that could be considered in the CPPA as well.

Further, the California code establishes a level of fiduciary care for platforms such that, if a conflict of interest arises between what is best for the platform and what is best for a user under 18, the children's best interest must come first. This is consistent with the recommendation of former commissioner Therrien and others in these hearings about including language around the “best interest of the child” in the legislation.

● (1550)

The CPPA should contemplate requirements for how businesses use children's data, considering the child's best interest. For example, use of children's data could be limited to those actions necessary to provide an age-appropriate service.

As I argued in my Policy Options article in January 2023, we need a collaborative approach that includes lawmakers and policymakers from all levels of government, coordination with global privacy laws, engagement with parents and coordination with educators. For this approach to work, the law needs to strike the balance between privacy and innovation. We want laws that are flexible enough to last so that technology can evolve, new business ideas can succeed, and children can be innovators while growing up in a world that recognizes their special needs and rights.

[*Translation*]

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

I'll now give the floor to Mr. Guilmain.

Mr. Antoine Guilmain (Counsel and Co-Leader, National Cyber Security and Data Protection Practice Group, Gowling WLG, As an Individual): Mr. Chair, committee members, thank you for inviting me to comment on Bill C-27.

Although I'll be testifying in English today, I'll answer your questions in either French or English.

● (1555)

[*English*]

I'm co-leader of the national cybersecurity and data protection group at Gowling WLG. I'm a practising lawyer called to the bars of Quebec and Paris. My evidence today represents my own views. I'm here as an individual, not representing my law firm, clients or any third parties.

Much of my legal career has focused on comparative analysis of legal regimes across the globe, advising clients on their compliance obligations in the jurisdictions in which I am qualified to practice.

Bill C-27 presents a tremendous opportunity to modernize Canada's federal privacy regime. It is possible, and indeed essential, that Canada protects the rights and interests of the public while facilitating competition, investment and ambitious innovation.

Many of the proposals in the bill are highly impactful, but I will focus my comments today on the consumer privacy protection act and two areas in particular that I consider to be of great importance. First are lessons learned from Quebec's law 25.

The majority of the provisions under law 25 came into force in September 2023. Over the last summer, Gowling WLG, in collaboration with the Interactive Advertising Bureau of Canada, conducted a readiness survey of over 100 organizations regarding this new law. The results of the survey were clear. Industry was ill-prepared for such an implementation. Specifically, 69% of the respondents expressed a need for greater clarity, and 52% indicated that they lacked sufficient resources. This also highlights that the compliance burden for SMEs is especially high.

There are four specific learnings from Law 25 that I wish to highlight today.

First, Bill C-27 should not exceed standards set by the EU general data protection regulation. For example, legitimate interest is a flexible legal basis for processing, but it must always be justified and documented in a separate assessment under the GDPR and under other global laws. A similar standard could apply in Bill C-27.

Second, Bill C-27 should not rely on future regulations to substantiate each requirement. This is a recipe for delays and uncertainty. For example, in Quebec, anonymization is currently regarded by the regulator as impossible because the regulations are not yet in place.

Third, Bill C-27's timeline for implementation should be sufficiently long. Based on experience from law 25, implementation should be at least 36 months after the bill becomes law.

Finally, Bill C-27 should be aligned with law 25 on key concepts, including around the legal bases for processing data and legitimate business exceptions. This is especially important when it comes to children's privacy.

I'm a father of two young children, so protecting children in the digital economy is important to me personally, and it's a subject that I engage with regularly in the course of my work. I believe amendments to Bill C-27 are necessary to ensure that minors' data is reasonably, meaningfully and consistently protected.

I wish to highlight four key topics for consideration.

First, as opposed to the GDPR, Bill C-27 lacks a threshold for determining when services are intended to target children. Practically, organizations will not be able to remain age-blind and will therefore have to ask the age of users each time they engage with them, to the potential detriment of user privacy interests and data minimization.

Alternative legal bases for processing should be available, depending on the maturity process of the individual. Specifically, legal capacity should be a baseline for assessing legitimate bases as opposed to the age of majority alone.

The process for collecting parental consent can be extremely complicated. Bill C-27 should set a specific age at which parental consent is required. Under 14 years of age seems the most reasonable standard.

Finally, the concept of the best interest of the child should be positioned as a key determinant of how minors' personal information should be treated, rather than relying primarily on the concept of express consent.

With the chair's permission, I would be pleased to submit a copy of the survey report for the committee's consideration, as well as a short written brief in French and English on the issues I've addressed in my opening remarks.

I wish to thank Michael Walsh for his assistance in preparing this material.

Thank you. I look forward to answering the committee's questions.

[*Translation*]

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

Lastly, I'll now give the floor to Mr. Arbuckle.

Mr. Luk Arbuckle (Chief Methodologist and Privacy Officer, IQVIA Solutions Canada Inc.): Thank you.

I'm very pleased to have been invited to participate in the work of the House of Commons Standing Committee on Industry and Technology on Bill C-27. I hope to be able to answer your questions on privacy and artificial intelligence services and technologies.

Although my opening remarks will be in English, please know that I will be pleased to answer your questions in either French or English.

● (1600)

[*English*]

My name is Luk Arbuckle. I am chief methodologist and privacy officer at Privacy Analytics, an Ottawa-based IQVIA company employing over 100 privacy experts.

My role at Privacy Analytics is to ensure that our company and our global clients are aligned on the practical applications of privacy-enhancing technologies and to inform our practices based on current guidance and emerging methods. I also provide guidance on the practice and risks of applying artificial intelligence in real-life applications. My role has been largely informed by my time as director of technology analysis at the Office of the Privacy Commissioner of Canada, when I also drafted guidance on anonymization for the office.

Privacy Analytics operates as an independent entity within the global IQVIA group of companies, so that we can provide both IQVIA and our global clients with services and technology for the safe and responsible use and sharing of data. The Privacy Analytics platform has been deployed globally to protect the privacy of close to one billion patients. For example, our software has enabled safe research that improves cancer outcomes for patients through the European oncology evidence network and the American Society of Clinical Oncology's CancerLinQ. We have also worked with multiple government agencies in Canada, Europe, the United States and globally to implement safe data access models that enable faster data access, promote research and innovation and implement data-driven decision-making.

It is against this backdrop that I wish to provide comments today. In particular, I will provide a perspective on the importance of health data and analytics for Canadians. Health care-related research is increasingly driven by analyses that draw from real-world evidence to reveal the effectiveness of treatments beyond the clinical trial phase. The success of that approach is predicated on the availability of the necessary data from various sources within the relevant health care system and on the ability to analyze data across different health care systems.

For Canada to take part in this new frontier of health care research, it is important that we prioritize a responsible data access model that strikes the appropriate balance between privacy and having useful data for the intended purposes. We also need a data protection framework that allows for efficient and effective data sharing and collaboration with stakeholders from all over the world, including the United States and Europe. As COVID-19 has shown, it is crucial that Canada stays active and competitive in life sciences. This means developing an approach to privacy that supports local research and innovation and allows health care research in Canada to align with efforts outside of the country.

I will only summarize three recommendations in my introductory remarks and invite you to consult IQVIA's full-length comment document on Bill C-27 for additional comments and details.

Recommendation one is to consider a reasonableness component within the definition of “anonymize”. The use of anonymized data in health care analytics is a key element in the research and innovation activities that help drive Canada's health care future. Canada's diverse group of health care stakeholders use anonymized information to identify inefficiencies and allocate resources more effectively, to speed up the development and approval of new treatments and to understand the needs of patients and health care professionals. Such uses of anonymized information contribute to better health outcomes and other notable benefits.

Including a reasonableness component within the bill's definition of anonymization would align better to other Canadian frameworks, such as Quebec's law 25 and Ontario's PHIPA. A reasonableness approach would also align better to the growing consensus in the academic and technical literature regarding the need for a realistic framing of risk in describing anonymized information. Take, for example, the risk-based international standard for an anonymization framework, technically known as ISO 27559. This technical standard was developed by experts from around the world and is consistent with the draft guidance I produced while at the OPC.

Recommendation two is to consider expanding the consent exception for “socially beneficial purposes” to include private sector organizations. A more principled approach would be to enable responsible data sharing between a broader range of actors while also mandating adequate oversight and data protection best practices.

Recommendation three is to consider a consent exception for external research, analysis and development purposes. Removing the internal qualifier would be a more beneficial approach, as it aligns with existing guidance and would enable a more useful model for health care research and innovation.

With that, I would like to thank the committee again for your time and for the opportunity to speak with you today. I strongly believe that it is possible to safely and responsibly use and share data in ways that protect privacy while driving innovation for the benefit of Canadians. I look forward to the continued discussions.

[*Translation*]

I will remain at your disposal during the discussion.

Thank you for your attention.

[*English*]

The Chair: Thank you very much to all of you.

To start the discussion, I will now yield the floor to Mr. Vis for six minutes.

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

Ms. Gordon, thank you so much for your comments. Thank you, all. All of the testimony today was amazing.

Ms. Gordon, you mentioned your three kids, and that's sort of what's driving me, with my three children as well, in the work we're doing to make sure this bill is done right and children's privacy is protected.

I've asked other witnesses questions on proposed section 9 of the bill, on privacy management programs. In some cases, what I'm hearing from your testimony is that in addition to having management programs, especially in relation to children, we need to be prescriptive in some aspects of the bill.

Would you support amendments to proposed section 9 or other additions to the legislation that are prescriptive, specifically in the case of children? Maybe proposed section 9 in its current form could apply broadly to privacy concerns, providing protections and making sure that businesses are providing those protections in the products they're producing, but what do we need to do specifically with respect to privacy management programs as they relate to children?

● (1605)

Ms. Michelle Gordon: As I said in my remarks, I do believe the law can be more prescriptive in terms of making sure we get it right for children. That is something we've seen in other jurisdictions. They've done it separately in a different law with a specific children's code. I think we can make certain amendments to the law or have a separate regulation.

Part of the problem with a regulation, as Mr. Guilmain said, is that sometimes it takes forever to get there and to get that guidance, so it's not always best to leave it to regulation, but that is one way of doing it. I do believe there are ways of adding amendments and making them more prescriptive so we can get it right in the law.

Mr. Brad Vis: Instead of privacy management programs, then, would you support privacy by design, requiring businesses to create products that are designed to have privacy, say, for children as the first and foremost priority?

Ms. Michelle Gordon: I don't think they're two separate things. I think you can have privacy by design in a privacy management program.

Mr. Brad Vis: Thank you. That's what I was looking for, actually. That's very helpful.

How would you define sensitive information?

Ms. Michelle Gordon: I don't have a specific definition, but I do believe we should be able to give a non-exhaustive list of examples, similar to what we've done in law 25 in Quebec.

Mr. Brad Vis: Can you give us some examples of a non-exhaustive list? What would be included in that?

Ms. Michelle Gordon: Sure. Some examples we've seen are biometric data, health data, financial data and children's data. Those are the ones off the top of my head, but I could certainly submit some more examples.

Mr. Brad Vis: If we apply a non-exhaustive list, is there a risk of leaving out future technologies and having companies being able to break the spirit of the law by not having a certain form of privacy or sensitive information included?

Ms. Michelle Gordon: That's definitely a risk, but I don't think that's a reason not to do it right now. PIPEDA has worked really well for 20 years. There's always going to be modernization of laws, but I think it's important to try to get that list now, with the acknowledgement that there is the possibility of updating it as things change.

Mr. Brad Vis: Okay.

The U.K. model for privacy includes, as I believe the law in California does, certain thresholds. I believe the spirit of the law implies that children at different stages are able to make different types of decisions.

How would you see that type of prescriptive language being included in Bill C-27, which is before us today?

Ms. Michelle Gordon: I don't have any specific comments right now on prescriptive language. Again, that's something I'd have to go back to.

I know that's something my colleague Mr. Guilmain also referred to, so maybe he has comments on that.

Mr. Brad Vis: Would you like to comment, sir?

Mr. Antoine Guilmain: Yes. I would like to take a look at what is being done in Europe at the moment. Of course, the GDPR has been a change for them, and privacy, children's privacy, was a key consideration.

Because it's extremely difficult to provide prescriptive requirements, they instead relied heavily on the notion of “best interest of the child”, and this is working. The reason is that it's not a free pass saying, “You know what? We talk about children but there's nothing to be done.” Organizations need to have documentation regarding what they are doing.

There's a second aspect I would like to highlight. Of course, being a lawyer, I like clear definitions, but the notion of evolving concepts such as “best interest of the child” is important as well in laws, as opposed to very clear-cut concepts such as express consent, where essentially we would need to have express consent every time, regardless of whether the person is a teenager or under 13 years old.

I think this is what we are seeing across the world, because many Parliaments understand that we are living in a world that is constantly evolving and that we need future-proof concepts, and the “best interest of the child” is not moot. It's a good concept. At least that's my personal opinion.

● (1610)

Mr. Brad Vis: Mr. Chair, how much time do I have left?

The Chair: You have three seconds.

Mr. Brad Vis: I'm good. Thank you.

The Chair: I'll now turn to MP Sorbara for six minutes.

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

Thank you to all the witnesses for their testimony on a very important piece of legislation.

If I may, I'll go to Mr. Goldfarb for the first question.

Mr. Goldfarb, you mentioned in your remarks that “Canada is a leader in AI research” and that AI and data-focused tools are promising for economic growth but obviously must be utilized. In that vein, you published an article in September 2023 called “The Economics of Digital Privacy”. I was wondering if you could elaborate in terms of how Bill C-27 would impact innovation, and thus productivity, and thus our standard of living through Canadian businesses and the economy, please.

Prof. Avi Goldfarb: Thank you for the question.

There are two key forces at play here. The first force is that any time you regulate companies and start-ups, especially small businesses, they're going to require lawyers in order to do business. That's going to slow down what they're able to do. That's on the one side. On the other side, if there is no legislation in place, then potential customers of those companies aren't going to trust the companies. Even though the need to get legal advice—apologies to the lawyers in the room—is a real barrier for small businesses and start-ups, you do need legislation so that people can trust the companies they interact with.

In my view, this bill balances those two very well, with some minor exceptions that I've mentioned. It protects against the most severe privacy harms, so that we'll have more trust in what organizations do with data. That will, in turn.... On the set of regulations as described, yes, it is a bill that runs dozens and dozens of pages—you'll need expertise—but it is not so onerous that I would expect that the small businesses and start-ups that have a big opportunity with AI will have to shut it down.

In my view, on balance, this will position Canada well going forward for our ability to commercialize AI.

Mr. Francesco Sorbara: Going down that vein, in terms of comparing pieces of legislation in different jurisdictions, how would you characterize the framework in Europe—the GDPR—versus what's contained in Bill C-27 with relevance to the impact on innovation and the economy?

Prof. Avi Goldfarb: We have plenty of evidence that the GDPR, when and where enforced, reduced innovation, hurt the European software industry relative to the American software industry, and helped the largest companies, particularly in advertising technology, do better and better. There were real costs to the protection of privacy that happened through the GDPR.

When I look at how this bill was drafted, I think that in protecting privacy and thinking about and addressing the potential harms of AI, to me it's clear that it was drafted with an eye towards the need for start-ups and small businesses to compete on a level playing field with the largest companies. In my view, this bill is more innovation-friendly, particularly for small businesses and start-ups, compared to the GDPR.

● (1615)

Mr. Francesco Sorbara: Okay. That's good to hear, in terms of how the law impacts innovation and productivity, because we know that innovation is a very large piece of what AI is and what impact it would have on our economy and standard of living in our daily way of life.

Luk, my understanding is that you're a private sector firm. Is that correct? You're a privacy expert. When I jotted down a few notes from your presentation or your discussion, one thing you commented on was the “reasonableness” approach and a realistic framework of risk when it comes to anonymous information. Can you elaborate on that to non-privacy and non-AI experts such as ourselves, who are grasping the information that's put in front of us in this bill, and on how important this is to everyday Canadians going forward, realistically? Can you elaborate on what you meant there and contextualize it, please?

Mr. Luk Arbuckle: Yes. The word “contextual” is important here, as well, because that's kind of how we want to look at anonymization. We want to look at where we are using this information.

When Statistics Canada produces statistics or data that they make publicly available, the risks are very high because it's on the Internet. Anyone can access it. They also take data and put it in a research data centre. It's disconnected from the Internet. You have controls according to who has access to the data, how they can use the data and what they can come in or out of the environment with. The risks are much lower, so it's contextual in that sense.

The idea of a reasonableness standard is bringing that contextual piece to it. When we look at international standards, for example, they're primarily very scientifically driven by risks, and risks are never zero. Therefore, by looking at it in this contextual way, we can manage the threats and use other tools besides just aggregating and creating means, as was mentioned earlier. We can do things that are a little more sophisticated, and we can have strong environments that control that information.

Mr. Francesco Sorbara: Prior to entering this privileged and honoured job that we get to do, I worked in the private sector for a very long time, for a very large organization in the financial services industry. How would you explain your company's use and compliance with PIPEDA?

Mr. Luk Arbuckle: The technology we use, the sophistication of it, is compliant in the sense that we look at the best practices that exist. We look at international standards. We look at guidance that is being produced, and we ensure that the anonymization we do meets those standards.

We have guidance in Ontario, for example. We have the law itself, for example, in Quebec. We have a variety of jurisprudence, which is not in my area, of course. We look at the best practices in terms of technology. We monitor the literature and the landscape of what's happening, and we modify accordingly.

Mr. Francesco Sorbara: How much time do I have? Is that it? Okay.

Thank you very much.

The Chair: We might have some time at the end.

[*Translation*]

Mr. Lemire, the floor is now yours.

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

My thanks to all the witnesses. I think we're having a very high-quality meeting today, and I'm very grateful to them.

Mr. Guilmain, I'll start with you. I'm going to continue in the same vein as one of my colleague Mr. Sorbara's questions. According to a letter published on the committee's website, although the minister assures that the Quebec legislation will prevail in the province, Jim Balsillie, in particular, expresses concerns that, if Bill C-27 sets standards that are lower than those of Quebec's Bill 25, it could hinder innovation and jeopardize investments in the Quebec economy.

With that in mind, how do you assess the potential impact of Bill C-27 on Quebec's economic landscape, particularly on investment and innovation?

Mr. Antoine Guilmain: At the moment, conceptually, Bill C-27 is quite compatible with Bill 25. I would even say that, in many respects, Bill 25 is stricter than Bill C-27. I'll go further than that: Bill 25 is one of the strictest laws in the world. That has to be recognized.

In my practice, I work with international clients, whether they are based in the United States, Europe or Latin America, and today, they look at Bill 25 and say that it's really one of the most complicated laws to implement and that it's difficult to comply with it. That's not a good thing.

My position today, quite frankly, is that the two pieces of legislation are compatible. However, I think there are lessons to be learned from Bill 25. I took the liberty of quoting the European Union's General Data Protection Regulation, the GDPR, and I think that's a very interesting model for Bill C-27 to look at. That's really my position.

There are some very good things in Bill C-27. It should be noted that, from a legislative standpoint, it makes a very different change. Bill 25 amended existing legislation by patching things up a little. We tried to add an act dating back to 1994. The beauty of Bill C-27 is that it's unified. There really is a collective understanding.

So my comment on this is to say that looking at Bill 25 as a yardstick may not be the best approach, in my humble opinion.

● (1620)

Mr. Sébastien Lemire: Thank you for your answer.

In that case, what amendments would it be worthwhile to make to Bill C-27 to ensure better compatibility?

I'm particularly sensitive to the need to have an environment conducive to innovation and investment. In the current context, is there a risk of establishing standards that could undermine investment and innovation in Quebec?

Mr. Antoine Guilmain: There's a fairly fundamental difference. As you know, when it comes to privacy, the notion of consent is central. It's all about consent. We're talking about either express consent implicitly or an exception to consent. That's how Bill C-27, the current federal act and the Quebec act are built.

Currently, Quebec's approach is very different from the rest of Canada. In fact, it decided to enshrine in law that, when it comes to the collection of personal information, consent isn't always required, provided that the reasons for collecting, using or communicating personal information are disclosed. This was recently confirmed in the guidelines of the Commission d'accès à l'information du Québec.

What does that mean in concrete terms? It's very theoretical, but it's not that theoretical. When you visit a website, you are “attacked” by various methods of consent. That's what we want to impose on children. As adults, our ability to concentrate is very limited. Personally, I have a full-time interest in this, and I don't read everything.

Quebec has decided to take a different approach: we don't force people to give express consent, to click, we just give them the information, and then they can continue with the process. This aspect of transparency is unique to Quebec.

At the moment, the federal legislation, as drafted, seems to indicate that a positive gesture should always be made in certain cases. I think that's a pretty significant difference. Again, not a bad thing. In fact, we're a different approach to the problem. We're providing a little more transparency, a little more control, instead of forcing people to consent in an almost fictitious way.

Mr. Sébastien Lemire: I'd like to ask you some brief questions about the delays in passing Bill C-27, since you've opened the door in that regard. Is there an urgency to act? What would the consequences of that be, if we took our time, in a parliamentary context like ours? What do you think about the government's delay in enforcing the act?

Mr. Antoine Guilmain: I'd first like to mention that our federal legislation, the Personal Information Protection and Electronic Documents Act, PIPEDA, is a quality piece of legislation. I wouldn't say that there's an urgent need to act, but that's a very personal opinion. There are fairly broad concepts in PIPEDA that already allow companies to do very good things. We aren't in a vacuum at the moment.

That said, Bill C-27 is very ambitious. I'm talking about the part that deals with the protection of personal information. We shouldn't underestimate the time it will take to adjust the processes. Let's not forget that companies had to grapple with Quebec's Bill 25 a few months ago and complied with it last September. It was a real inhouse effort.

I think there's an interest in avoiding a duplication of resources, at the risk of creating a kind of fatigue on the part of companies with regard to requirements. Businesses will no longer understand the message being sent to them. I think it's important to keep in mind the significant transition period.

I don't think there's an urgent need to act, but that's my very personal opinion.

Mr. Sébastien Lemire: What about aligning with the European Union?

Mr. Antoine Guilmain: In terms of aligning with the European Union, I must say that it will require an analysis that may take years. Japan recently received a suitability decision and is considered a good country for the transfer of personal information. This is the result of years of work by the European Commission.

I think Bill C-27 is a very good bill in terms of complying with European standards, in this case the European Union's General Data Protection Regulation. There are a lot of “Canadianized” concepts, if I may say so. It's worded a little differently, particularly when it comes to sensitive data. I still think that Bill C-27 is a good bill in that regard, apart from certain aspects on anonymization and the legal basis for handling personal information, as I mentioned.

● (1625)

Mr. Sébastien Lemire: Thank you very much.

The Chair: Thank you, Mr. Lemire.

Go ahead, Mr. Masse.

[*English*]

Mr. Brian Masse (Windsor West, NDP): Thank you to the witnesses for being here.

Maybe I'll go across the board here.

For the Americans, Biden's executive order gives the administration, from the top down, more control and ability. Basically, it removes Congress, in many respects, from making decisions, and the executive order is almost like an order in council here. We were fortunate to be in Washington, and when our analyst was there, she clarified that as well. It was an interesting point that we didn't realize—the extent to which it has been removed from the halls of Congress and, to some degree, the Senate.

I'm wondering what your position is with regard to how we deal with the United States' executive order coming from the administration, as it really will be a top-down approach that they're going to have. How do we have any type of consistency with that in our country as we go through these hearings here?

Ms. Gordon, I don't know if you want to start, and then we'll move across the table here.

Ms. Michelle Gordon: I'd have to think about that for a minute, so perhaps one of my colleagues can start.

Mr. Antoine Guilmain: I'm going to be very blunt. I'm not equipped to respond to your question.

Mr. Luk Arbuckle: It's an interesting question. Are we talking about the executive order on artificial intelligence?

Mr. Brian Masse: Yes. I'm sorry. I should have been more specific.

Mr. Luk Arbuckle: It's okay. I just wanted to check. There may be another one. You never know.

It's interesting. There's a lot of activity. There's a lot of work in the U.S. The National Institute of Standards and Technology, for example, has put together really good work on AI risk frameworks and how to manage it. We've heard a lot of good things in the executive order, so from a technology perspective I think it's exciting to see the talk of safe, trustworthy and responsible AI. Regardless of the procedure—I can't really speak to that—it's exciting to at least see there's a big push.

Canada is known for privacy by design, for example, so we have an opportunity as well to take the lead and to do things in AI. As was mentioned earlier, we have researchers who have done tremendous work, really, bringing this forward. Regardless of the procedure of how it was done, I do think it's interesting that they're pushing it so much.

Mr. Brian Masse: If you don't have comments on this, that's okay. The reason I outlined the procedure is that it's going to come right from the president now, and it actually bypasses, to some degree, the oversight of Congress and the Senate.

That was the way they approached it. They almost handed over the elements to the president, whereas we're still in a committee here. We still have to go through a legislative process, and then we have to send this bill to the Senate, and then we have to get it done. At the same time, we don't know exactly if it's going to be somewhat consistent with the United States. We have to somehow figure that out. It's almost like, if we want to have something similar or comparable, we need a treaty in some respects for this.

Of course, we want our sovereignty, but I guess what I'm worried about is that.... If we are significantly different from the United States, does that affect our capabilities to retain investment and AI here, or does it put us in a better position, potentially? I'm wondering what your thoughts are, because we could have two different models in North America on how to deal with AI. Do you have any thoughts on that?

Mr. Antoine Guilmain: A general thought would be that I don't see it as a particular problem, because that's what we see. Having seen many laws across the world, it's never unified. I think this is something impossible. Even in Canada, we have the private sector laws in B.C., Alberta and Quebec, and the federal statute at the moment. They are not unified; they are different.

What is important is interoperability. It's the ability to talk between the laws. I think that is something we should be seeking, as opposed to having exactly a carbon copy, potentially, of what is being done in the U.S. The same would apply to Europe. I think it's just looking at what they are doing and making sure our concepts are flexible enough to essentially talk with the potential legal regime that is being adopted in the U.S.

Mr. Brian Masse: Okay, that's a good distinction.

What I worry about, coming from my world, is that for years we had two different sets of bumpers on cars. It stopped the ability to talk and to trade, and we actually had some companies doing duplicate stuff. I don't know enough about this as to whether or not it impedes.... Unlike the European Union, in many respects, we have a lot of North American partners and subsidies back and forth. I'm just trying to figure that out.

How much time do I have, Mr. Chair?

The Chair: You have about a minute and a half.

Mr. Brian Masse: Just quickly, does anybody have any comments on the issue of the Privacy Commissioner's recommendations? Are you in favour of the Privacy Commissioner's recommendations or opposed to them? Is there anything that is glaring there? Does anybody have any comments on that?

● (1630)

Mr. Antoine Guilmain: Do you mean the 15 recommendations?

Mr. Brian Masse: Yes.

Mr. Antoine Guilmain: If I can opine on one aspect, there are some interesting ideas. I think there's a will to add an accountability obligation for companies. I think that's something that is being proposed. I have some caveats in this regard, having seen what is happening in Quebec at the moment, especially for small and medium-sized companies, which are really struggling to have accountability documentation for everything.

It could be a good idea, to the extent that there are thresholds. I think that is the key aspect in these kinds of laws, having the notion and the principle but not forgetting the exception and the thresholds. That is my top potential concern with that recommendation.

Prof. Avi Goldfarb: Just to add to that, I think it's important to recognize there are trade-offs here. As we make the privacy rules in this legislation stricter, in many cases we're going to get less innovation, particularly from start-ups and small businesses. The big ones will be fine, but the start-ups and the small businesses will have a harder time as it gets more difficult for them to collect and organize data.

To the extent that those recommendations are accepted, keeping an eye on the situation and making sure we don't overburden those small businesses and those start-ups is important.

Mr. Michael Beauvais: To quickly respond to Mr. Masse's question about the executive order, I would note that insofar as you're able to put things into secondary or delegated legislation, you would provide an opportunity for some type of harmonization. However, it's a tricky question of balancing what should be in primary legislation versus secondary legislation.

Thanks.

The Chair: Thank you very much.

MP Williams, the floor is yours.

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

I want to stay in the same vein. I think this is a great discussion.

We obviously believe in privacy as a fundamental right, but at the same time, businesses have to be able to collect and use data. We're in a unique situation right now with Bill C-27 because the GDPR has just come into place with some of their.... I hate to call it red tape, but it's the processes in which businesses, small and otherwise, have to follow those rules.

We're trying to look for good amendments in this bill that obviously make sure that privacy is held as a fundamental human right, but also protect businesses from the overburden and the policies and procedures that are going to weigh on businesses' ability to do business as well as collect and use data for good.

I'm going to start with Ms. Gordon.

What can we do in this bill to ensure that this collection and the consent models are easy for businesses while also protecting privacy? What have we learned from the GDPR?

Ms. Michelle Gordon: That's a really good question.

I generally support the new exceptions to consent in Bill C-27 , which are similar—slightly different—to the GDPR. I agree that the application of the legitimate interest exception, whether as a stand-alone right or as an exception to applied consent, will help a contextual analysis and will help nurture innovation and allow for a difference between...how organizations look at their programs and at accountability and transparency.

Mr. Ryan Williams: Would you support an amendment to the bill to exempt businesses of a certain size from filing requirements?

Ms. Michelle Gordon: Again, that's something I'm not entirely qualified to comment on right now.

Mr. Ryan Williams: Thank you.

Mr. Guilmain, could you respond to that question specifically, but also comment on the burden to business?

Mr. Antoine Guilmain: I want to start by saying something. It sounds like a paradox, but I believe it is true. More prescriptive requirements will not necessarily lead to more protection of personal information. I think it needs to be heard. It's not that because we are adding a lot of burden on organizations, it's going to be better for the public. I want to start with this statement.

That said, I will give you an example. When we hear the words “legitimate interest”, the perception may be just to say, “Well, it's a free pass. You do whatever you want. There's no consent, so you do whatever you want.” The fact is that in the GDPR, there is always documentation.

To your second question, about small and medium-sized companies, I don't think it makes sense to have different obligations based on the number of employees. What matters is the sensitivity of the information and the volume of the data. This should be, from that perspective, the trigger to essentially say that they need to have more documentation in place to explain what they are doing. These should be the triggers. This is my humble opinion.

Again, I don't think we should be afraid of using some terms. Also, “exception” doesn't mean that there's nothing in place. As a matter of fact, at the back end, what I'm seeing is that there's a lot of documentation in this regard.

● (1635)

Mr. Ryan Williams: To ask that specific question again, would you support amending the bill to exempt businesses of a certain size from filing requirements?

Mr. Antoine Guilmain: No.

Mr. Ryan Williams: You'd require all businesses to fill out that documentation.

Mr. Antoine Guilmain: It would be to the extent that we are adding sufficient triggers based on the types of information.

These questions were raised as part of law 25. Clearly, the question was, what do we do with a company that...? Let's say a convenience store in La Tuque has some personal information. What do we do with this? The fact is that the convenience store in La Tuque potentially will have non-sensitive personal information. As such, it should not potentially need to have a privacy officer. That makes sense.

However, let's say we have a growing company with 20 people building a very interesting AI model with biometric data or health information. Then I think it would make sense to potentially have some obligation.

Again, this needs to be proportional. I want to give my opinion. I don't think that the number of employees makes sense. Even the revenue is not a good threshold, from my perspective.

[*Translation*]

Mr. Sébastien Lemire: That convenience store is in Minister François-Philippe Champagne's riding.

[*English*]

Mr. Ryan Williams: Would other witnesses like to weigh in?

Go ahead, Mr. Goldfarb.

Prof. Avi Goldfarb: Creating thresholds based on the number of employees creates incentives for businesses to stay small. While there is a desire to have these additional burdens on businesses, we have to recognize that there is a trade-off if doing so depends on the number of employees, because what you're telling businesses is that you don't want them to grow.

Mr. Ryan Williams: Mr. Arbuckle, do you have anything to add?

Mr. Luk Arbuckle: I am very supportive of all the comments that have been made. We had this debate when I was at the OPC. We did a public consultation, and the question came up about an AI start-up processing terabytes of data. It's not about the size; it's about the amount of data and the kind of data.

To your earlier question as well, I'll just add to some of the comments I made earlier about consent exceptions. I think there is an opportunity to align more closely with the GDPR in the sense of making it available to a broader range of organizations—small, large, etc.

When we're dealing with health data, for example—and I've seen this while working across Canada—we have some small, vulnerable population groups, and they can't anonymize that information with such a small population, so how do we bring that data together? How do we bring health care data together? It's partly through some of these current provisions where there is de-identification. We take out the person's name and we put in a pseudonym, but we still link and then produce really interesting, important statistics.

That's the one thing I wanted to bring forward.

Mr. Ryan Williams: Mr. Beauvais, go ahead.

Mr. Michael Beauvais: The point about record-keeping obligations is interesting. To my knowledge, the only olive branch the GDPR hands small and medium-sized enterprises is indeed concerning their record-keeping obligations.

I would note that in the case of a children's code, which Ms. Gordon and I have spoken about, that can actually be very useful for helping businesses, because it provides them, in a way, with a starter manual for thinking through how they should design their products and services that are directed to children. You can raise protections while also being clear and helping businesses in terms of compliance.

The Chair: Thank you.

Mr. Turnbull, the floor is yours.

Mr. Ryan Turnbull (Whitby, Lib.): That's wonderful, Chair, and what a nice surprise it is to have a meeting with such great witnesses and without the Conservatives moving a motion to disrupt the meeting.

It's really nice that we get to have you here today.

Mr. Goldfarb, I'll start with you.

I know you mentioned an overly broad definition of AI and you cited some examples, such as regression analysis and some others, that might be captured within the definition of AI currently. I'm wondering how you might narrow the definition. I'm not sure if you have specific suggestions on wording or amendments, but I'd be interested in hearing your thoughts on that.

● (1640)

Prof. Avi Goldfarb: Absolutely.

In my speaking notes, I have a footnote, so I'll just read that: “the use of a genetic algorithm, a neural network, machine learning or another AI technique in order to generate content or make decisions”.

The current definition is about any prediction model—and an average or a regression is a prediction model. The definition of an AI technique will evolve over time. What the use of “another AI technique” does is allow for the flexibility of technology to change over time, but it doesn't start regulating statistical technologies that have been around for centuries.

Mr. Ryan Turnbull: Okay. Thank you.

I know we've also had a running theme here about perhaps the compliance burden being fairly high on SMEs.

Mr. Goldfarb, you talked about a trade-off or trade-offs—I think it was in the plural. You said that privacy is not free but Canadians care about it. I think many of us probably agree with those sentiments.

What I want to understand is how we can reduce that burden without going too far. I've been thinking about this as a balancing act—as many pieces of legislation are—between the interests of different groups. There are some people who say that the fundamental right to privacy should supervene everything, but it seems as though we could go a little too far down that road and really stifle innovation and also cause undue compliance burden on small and medium-sized enterprises.

I know you spoke to that. I wonder if you could make any suggestions as to how to reduce that burden specifically.

Prof. Avi Goldfarb: My starting point is that I think this legislation already is at a good starting point. Where we are right now is good. My concern about the trade-offs would be if we're adding additional things.

That said, there are two pieces that I think are particularly important. The first one is some recognition by the commissioner of the burden on small and start-up businesses. Especially, right now, the cost is borne by the person audited, even if the commissioner finds nothing. That strikes me as very risky. If we have a commissioner who decides, for whatever reason, that a particular company, especially a small company or a start-up, deserves an audit and they go through that process, for the start-ups that work with the Creative Destruction Lab, that may very well kill the company. Some reasonable expenses, in my view, should be covered by the commissioner or by the government when the audit shows no evidence of a contradiction of proposed sections 6 to 12.

Mr. Ryan Turnbull: Okay. That's interesting. I hadn't thought of that before, but I can see your point that the risk of being audited or actually being audited, when it's proven later to be not initially warranted, could be very costly if the burden is on the small and medium-sized enterprises. I get that.

Mr. Guilmain, you also mentioned this as a sort of running theme in your opening remarks. You said industry was ill-prepared. You even said that the implementation time should be up to three years. I'm wondering what your thoughts are on how we get the balance right but also reduce the burden. I wonder if you have any more thoughts that you haven't been able to share on the trade-offs there.

Mr. Antoine Guilmain: Yes. I think there are two sub-aspects from my perspective.

The first aspect is the transition period. I think we should not undermine the fact that, even though there are already processes in place with PIPEDA and potentially with law 25, it does take time to have something that is meaningful.

I'm a lawyer, so I wish I could tell you that it's only a question of the papering aspect and just giving some policies and moving on. The fact is that privacy is much more than only legal professionals. I think there's an understanding internally in any organization to understand what is going on in terms of data flows and what we do to protect the information we have.

That's the reason why I tend to think that 36 months is the bare minimum. As a matter of fact, when we look around the world, that's what we are seeing. We saw with law 25 that 24 months was not sufficient. At the moment, companies are struggling very much to comply even with law 25, most of which came into force.

On the second aspect of your question, regarding what we can change, I will give you a simple example. If we go to proposed section 8 of the CPPA, it says, “An organization must designate one or more individuals to be responsible for matters related to its obligations under this Act.” I'll go back to my example of the convenience store in La Tuque. They have very little personal information. Their first question when they come to me would be, “Whom do I appoint? Who is my privacy officer?”

I think this is where it is problematic. It's not based on the size of the company; it's more a question of the volume and sensitivity of the information, the good news being that this threshold is present in Bill C-27 in some disposition. In particular, when I look at the privacy management program in proposed section 9, there is a caveat: depending on the “volume and sensitivity” of the information. I think the key aspect would be just to look at those absolute requirements and say, do we have a threshold based on the volume and sensitivity of the information? I think this could be a good exercise in the full version of the CPPA at least.

● (1645)

Mr. Ryan Turnbull: Thank you for that. That's great.

Mr. Arbuckle, I have a question for you, if I still have time.

Following up on my colleague Mr. Sorbara's comments, which I thought were quite good, in terms of the reasonableness component on anonymized data that you were talking about, what I want to understand better is what's at stake. I wonder if you could provide an example where the health outcomes would actually be potentially compromised.

I think what you implied to me was that if you were adding that reasonableness component to the clauses around anonymized data in the bill, you would in fact allow for that contextualization and perhaps a strong protected environment, in which case you could use that data for purposes that are beneficial. You spoke to health outcomes. Could you give us an example to illustrate?

Mr. Luk Arbuckle: Sure. We've even seen it in other jurisdictions. Basically, the best example is probably the one of small populations. When you want to bring data together and produce.... Basically, what is anonymization? It's producing statistics. We've heard means, aggregates, averages and stuff. That's essentially what we want to do when we talk about anonymization.

If we make the threshold such that it's a zero risk, and if I have 100 people.... If I take the average age of everyone in this room, you will say, “Well, it's not anonymized enough”, but who is going to be able to identify me from the average age in this room? That's the risk. You're going so far and you're saying, “Well, 100 people are not enough. We have to go to 1,000.” Suddenly, you cannot generate the statistics that we currently generate for things like.... In our submission, we included opioids and mental health. These are examples where it would be very hard to create the granular data to see trends over time in different age groups and in different provinces.

Mr. Ryan Turnbull: Thank you very much for that exchange. I found it very valuable.

Mr. Chair, I think I'm probably out of time.

The Chair: Yes.

Mr. Ryan Turnbull: Thank you very much.

The Chair: Thank you very much.

Monsieur Lemire, go ahead.

[*Translation*]

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

My question is for Prof. Goldfarb.

In recent weeks, some members of the Bloc Québécois have heard concerns from creators who think that the future artificial intelligence and data act, or AIDA, won't adequately protect their copyright. This issue is even more important in Quebec, where the arts, music and literature are at the heart of cultural and linguistic vitality.

What specific amendments could be made to the proposed AIDA to strengthen the protection of creators' copyright, particularly in a context where cultural and linguistic preservation is a priority?

[*English*]

Prof. Avi Goldfarb: From my read of the bill right now, it is not addressing AI and copyright.

I think there are important trade-offs to recognize in thinking through this. On the one hand, it's very important that artists and other people who create work get compensated for it. It is also important that we recognize that there has to be some aspect of their use.... When we, ourselves, read a document and then write something two or three years later, that document might somehow be in the back of our mind as we're drafting it up. We might cite that original person, or we may not, but we don't owe that person funds for copyright.

The first response is that, from my understanding, this bill does not address that. There are reasons to think that clarity will be good. Wherever we land, with a lack of clarity, it is going to be difficult for businesses to build AI systems, and it's going to be difficult for copyright owners to get compensated for their work. Clarity is good. As I understand it, it's not in this bill.

Second, I think it's important to recognize that some of the ways in which copyrighted work is input as data into the AI systems are very clearly related to the value of the copyright. If you ask it to write a song in the style of The Tragically Hip, it will. That's the style of The Tragically Hip, and that seems related to The Tragically Hip copyright. In contrast, if you ask it to create something that rhymes and somehow, in the dataset, there is some copyrighted work that rhymes, thinking through how every single copyright owner who's written something that rhymes should be compensated will be quite a nightmare.

● (1650)

[*Translation*]

Mr. Sébastien Lemire: Taking it a step further, to what extent will insufficient copyright protection affect cultural creativity? How can we learn from international best practices to mitigate potential negative impacts?

[*English*]

Prof. Avi Goldfarb: I was at a recent poetry reading, of all things, at an AI conference. The poet used AI to develop her poetry, and it was amazing and fascinating and a pleasure to listen to. That's creativity enabled by AI. That poet got to copyright her work. The other poems that were inputs into the overall database at that point did not get to benefit from their copyright.

The reason I tell that story is to recognize that for cultural creativity, going forward, there are reasons to want a very open use of these AI systems. There's incredible creativity coming out of these AI systems—not the [*Inaudible—Editor*], to be clear. One of the things I love about the bill itself is that it's so clear that humans make decisions and not machines, so the creativity is human creativity enabled by AI systems.

In the process, though, we need to make sure that when copyright is violated in a particular way—for example, it's clear that you were trying to mimic a particular artist's style—it gets protected.

[*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.

Federal parties are not currently included in the bill. Does anybody have any feelings on that and whether the inclusion of federal parties should be part of it? We were exempted from other legislation in the past. The do not call list is one exemption.

Does anybody have any feelings on whether federal parties should be part of the bill? It usually comes to the privacy commissioners and others.

Ms. Michelle Gordon: Other witnesses who testified here have said they should be included in the legislation. I agree with them and agree with their reasoning.

● (1655)

Mr. Brian Masse: It doesn't have to be exactly the same as the business sector either; it could be done in a different way. It doesn't have to be entirely the same, but I think there is an argument that could be made that federal parties should be part of this.

Mr. Antoine Guilmain: Yes. I would agree as well.

My only problem is—and maybe I'm a bit too dry—that the title of the law itself is “consumer privacy protection act”. The notion of “consumer” is misleading at this stage. I think it's something to emphasize, even though I don't disagree with the principle of potentially having federal political parties be subject to the law.

Mr. Brian Masse: Well, if you have been here long enough, you know that the titles of bills are often divorced from the reality of what they are.

That's a fair point, and I'm complimenting, not criticizing, your analysis of that.

Does anybody else have any thoughts on that?

Mr. Michael Beauvais: I know that Colin Bennett, among others who appeared before this committee, also raised this point. In light of big data political campaigning, I think it's very difficult to sustain a justification for why political parties should not be subject to data protection laws. I would certainly encourage their inclusion.

If there are specific concerns, a balancing can take place, in the way that data protection laws frequently balance with journalistic purposes and these sorts of things. If there are very specific concerns about campaigning and the political process and how data protection law can affect that, I think that should be considered in a very specific manner, but certainly as a big-picture item, I think political parties should indeed be subject to data protection law.

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

[*Translation*]

The Chair: Thank you.

Mr. Généreux, the floor is yours.

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

I'd like to thank all the witnesses. Their comments are really very interesting.

Mr. Guilmain, I'll turn to you.

I'll go back to the example you gave, the convenience store in La Tuque. We all understand that you chose that location, since the convenience store is in Minister François-Philippe Champagne's riding. Up until now, he probably thought he had a little private life, but with the convenience store story, his life has now become public.

I'm using your example to talk about small businesses across Canada. We know that 95% of businesses in Canada are the backbone of our economy. With this bill, we are addressing both individuals and businesses and entrepreneurs who will have to adapt to this legislation.

Earlier, you referred to a survey you conducted on Quebec's Bill 25. Nearly 70% of respondents needed more information or clarification on the act.

Do you think the process will possibly be the same for Bill C-27?

We're talking about consultations. You think this is a good bill, from what I understand. However, I must say that this isn't exactly what we've heard since the beginning of the consultations.

A number of people have told us that they weren't consulted. Representatives of organizations, who have appeared before our committee so far, have said that they weren't consulted. Some have told us that it would be preferable for them to be consulted. I think one of the witnesses said so earlier. He said that it would be good if there were more consultations.

Do you think it would be a good idea to hold more consultations?

We've been told on a number of occasions that we should normally, at the outset, separate the whole issue of artificial intelligence from that of privacy, because they are two completely different things.

What are the real or possible consequences of the elements that will, in a way, bury SMEs in bureaucracy?

Mr. Antoine Guilmain: If I may, I'll answer in three parts.

First, there is Bill C-27 in and of itself. I grant you, in my humble opinion, that part 3 and parts 1 and 2 are probably unrelated. That's a real problem. I won't hide the fact that, when I talk about the aspect of Bill C-27 that I like—it's always like that in a relationship, we like or we like less—I'm talking about parts 1 and 2, to be quite honest with you. That's the first thing. I think part 1 is a very good start. There are gaps. As I told you, it's not perfect in terms of compensation and the flexibility of consent, among other things. However, in my opinion, the bill is a very good foundation.

Second—and I go back to my earlier comment—I think there's a common sense rule with respect to this piece of legislation. It's just a matter of looking at the obligations in a very cold way. We have to ask ourselves some questions. I would like to come back to the example of the famous La Tuque convenience store, which, by the way, is being well advertised. I don't know if there are two, though. In any case, if I were the owner of this famous convenience store and I saw this text, I would wonder if it would help me in how I operate. Is this piece of legislation really going to change the way I do things? That is the objective. We really have to show businesses that we don't want to create problems for them for the sake of creating problems for them. We have to tell them that we want to help them focus their attention on the right things.

I gave you the example of the privacy officer. I don't personally believe that our convenience store needs a privacy officer. I think it's that kind of analysis that could really help small and medium-sized businesses. We have to put ourselves in their shoes and ask ourselves whether, based on what we see, based on non-sensitive data…. Again, I think this is an important element, because small and medium-sized businesses have a voice that is heard, obviously, but it will depend on the data. Data is really the key. However, I think you have to look at some of those things, and obviously that has been taken into account in some provisions and not in others.

Perhaps we need to make an effort to be consistent and to ensure that this aspect is truly taken into account. That could help, I think.

● (1700)

Mr. Bernard Généreux: While I'm at it, since you're a lawyer, I'm going to ask you about a proposal that was made in the legislation to set up a tribunal.

If that question is of interest to Mr. Arbuckle and Ms. Gordon, they can also answer it.

Some have told us that establishing a tribunal should be set aside. For example, Mr. Balsillie, from the Centre for Digital Rights, said that it was a dog's breakfast, that it would do absolutely nothing. Other witnesses have said that this will delay the process.

What do you think?

I'd like to hear from all three witnesses.

Mr. Antoine Guilmain: I don't agree with that statement, quite frankly.

I think you have to look at the nature of the organization. The Office of the Privacy Commissioner was created as an ombudsman would have been, and that's its role. The Privacy Tribunal would have a different, purely jurisdictional role. I think that's an interesting approach.

I'd like to look at what's being done in Quebec. You might be interested in that. We have the Commission d'accès à l'information du Québec, which wears two hats. It has general oversight over everything to do with complaints, recordings, and so on. It has a jurisdictional section, where administrative judges render decisions.

I find that an element of complexity. I think it's good to have two distinct entities. That's my own point of view. I don't think that's a bad idea per se.

Mr. Bernard Généreux: What do you think, Ms. Gordon?

[*English*]

Ms. Michelle Gordon: Just on the topic of the tribunal, I do support that idea. I think the current role of the Privacy Commissioner.... That office has done an incredible job, but it wears many hats. The commissioner wears the hat of an advocate and of an educator and does investigations, but what's always been said about that role is that it has no teeth, that whoever is in charge doesn't have teeth to implement fines and issue fines. By having the separate role of the tribunal, that will allow for a more robust legislative process and allow the hats of the commissioner to be separate.

[*Translation*]

Mr. Bernard Généreux: Mr. Arbuckle, I don't think you're a lawyer, but do you have an opinion on that?

Mr. Luk Arbuckle: No, not really.

The Chair: Thank you very much.

Mr. Gaheer, you have the floor.

[*English*]

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

Thank you to all the witnesses for making time for the committee.

My questions are for Mr. Guilmain.

I think you've answered this piecemeal, but I wanted to give you the question so you can approach it: How does the CPPA align with other privacy and data protection regimes? I want you to focus on the GDPR. Given your expertise, how do you think it compares overall?

Mr. Antoine Guilmain: There are a couple of things.

I think the first aspect is that the idea of asking the organization to explain what they are doing on the privacy side is very similar to the GDPR, to what we are seeing at the moment. I think it's positive in itself.

The second aspect is that there are some interesting legal bases and ways of making legal the processing of personal information, and I will give the example of legitimate business exemptions. Unfortunately, I want to say that they don't go as far as the GDPR does, and I think this is something that should be considered, at the very least.

The third aspect—and I think it's important—is that the CPPA places privacy as a cornerstone for society, very similarly to the GDPR. I want to be clear that the GDPR has been a shock in Europe in itself. Everyone knew about it. It was an earthquake. I tend to think that the CPPA in its current version, with some improvements, could have the same effect, potentially pushing the organizations to do even more on the privacy side, relying on what they've been doing.

I think those are the elements that are common between the two regimes.

● (1705)

Mr. Iqwinder Gaheer: Thank you.

How was the GDPR received by businesses in Europe? Was there a warm reception? Were they able to get on board and comply?

Mr. Antoine Guilmain: The first months were rough. Let's be honest. I think that everyone was just trying to adjust. We have to keep in mind that it was in May 2018, so it was the first big change in the world. Just to be clear, it's been the same across the world. Brazil recently adopted its own privacy laws, Singapore.... It really was the beginning. Let's put it that way.

Then, eventually, I think the regulators, in consultation with the organizations, were able to make sure that the organizations understood what was expected from them. I think that at this stage, there's a big aspect of expectation, because the companies want to do well. That's what I see in my practice. They want to comply. No one wants to say, “Well, you know what? We don't want to comply.” The problem is always in being clear regarding the requirements and being reasonable as well.

On the GDPR, at the moment in North America we are using the GDPR as a gold standard in transactions between U.S. and Canada. We are using language from the GDPR. Clearly, it shows that it's been a success for Europe, if we are being honest. That's my position.

Mr. Iqwinder Gaheer: In your second point, you mentioned that the exception in the CPPA doesn't go far enough. Could you speak about exceptions generally and maybe about the business purpose exemption in particular?

Mr. Antoine Guilmain: Yes. I know that you've been discussing this notion of legitimate interest. When we hear "legitimate interest", it sounds like a free pass to do whatever we want, but I want to emphasize that if you look carefully at the CPPA, there is always an aspect of assessment, of explaining why we can actually rely on legitimate interest.

The fact that we are limiting.... For instance, for influencing the decision, we don't want to use legitimate interest. That's what we have at the moment in the law. I think it's a mistake, because the influence could be bad or it could be good. I will give you an example. For instance, my children are online on social media. They can see targeted advertising, contextual, without any context, regarding alcohol or something I don't necessarily like as a parent. I'd prefer for them just to have specific tailor-made advertising for children. That's what I'd prefer. I think legitimate interest could be used.

I think this is the perfect segue between legitimate interest and children. I think those are topics that you've been discussing a lot lately, as I understand. I think potentially legitimate interest is not evil. I think it's a question of documentation. I'm going to give you the word that we use in Europe: legitimate interest comes with LIA, legitimate interest assessment. This is a document, a report, explaining why and how you are relying on these legal pieces. I think the same could be done here.

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

[*Translation*]

The Chair: Thank you.

Mr. Lemire, you have the floor.

Mr. Sébastien Lemire: Isn't it at the end of the second round?

The Chair: You're right.

Thank you. I'm lucky to have you as vice-chair, Mr. Lemire, to call me to order.

Mr. Perkins.

[*English*]

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

This has been fascinating, as has been the testimony on the whole thing.

Dr. Guilmain, you have two Ph.D.s, as I understand it. You've pretty much earned the "Dr." You have a very impressive background.

You seem to be getting all the popular questions here. I'd like to talk to you about two things. One is the issue of consent, which we have raised before. I've raised this in the committee before with other witnesses—the famous thing that happened with Zoom in the summer. I know from your résumé that you seem to have done some work in the past for Meta.

This is from section 15.2 of Zoom's consent clause on privacy that we all click—and even most lawyers click, too—without actually reading most of it. It says, "You agree that Zoom may modify, delete, and make additions to its guides, statements, policies, and notices, with or without notice to you, and for similar guides, statements, policies, and notices applicable to your use of the Services by posting an updated version on the applicable webpage."

To me, that doesn't sound like consent. It sounds like it's changing the terms without your consent. Is there anything in this bill that prohibits that practice?

● (1710)

Mr. Antoine Guilmain: I'm going to emphasize the obvious. I'm here in my personal capacity, to start.

The second aspect is that what you are showing at the moment is the limits of consent. That's what it is. It's essentially showing a big chunk of text and expecting the individual to consent. That's the reason exemptions to consent are interesting, because you will actually focus on the important moment of a data flow. Essentially, if you want an express consent on biometric data, then you're going to ask for consent.

Those kinds of things potentially could have been, in my personal view, captured by the notion of legitimate interest. If the regulator, the OPC, has any questions, then it can knock on the door and ask, "Why are you doing this? Show us the assessment."

That's the reason why consent, to me, is not necessarily the solution. It's not bad. I think, globally, there's a consensus. Everyone understands consent. We like the notion. I think it sounds good. At the same time, it has limits. If we want meaningful consent, then we should focus on express consent in limited situations. Otherwise, we will spend our time consenting and not meaningfully consenting. I think this is my—

Mr. Rick Perkins: I'm sorry to interrupt, but I have limited time.

Proposed subsection 15(5) says that implied consent can be used, and you've talked about proposed subsection 18(3). When you pile all those up with proposed section 5, the "Purpose" section, which says that a company's interest is of the same value as an individual's right to the protection of privacy, doesn't that weigh everything in my favour, for me, as a former marketer, to be able to use and to do what my company needs most, over your personal interest?

Mr. Antoine Guilmain: That's not necessarily the case, because the balance is always in thinking about the rights and interests of the individual. It's not something that you do in a vacuum. These are analyses of proportionality and of necessity. It's a long assessment. It's not a two-pager. I think it's not only that.

Mr. Rick Perkins: Thank you, Dr. Guilmain.

Mr. Chair, I'd like to propose a motion, because I was poked by the bear. I wasn't going to do this, but I'll do it now, anyway.

I move that, pursuant to the request for documents passed by the committee on November 21, 2023, the committee order the Minister of Innovation, Science and Economic Development to produce unredacted copies of the Stellantis-LGES battery plant contracts to members of the committee in both official languages—in other words, get it translated—by Tuesday, November 28; further, that the committee pause the study of Bill C-27 until the contracts have been circulated.

The reason, Mr. Chair, for doing so is that we all know the government has hired, over the last few years, another hundred thousand officials. Surely, they can get it translated if the contracts weren't presented in both official languages. It surprises me that the government would not have contracts in both official languages before signing them.

I request that all efforts be made on this critical issue, where such a large government subsidy is involved and where there are such conflicting public reports about what's going on, so that we get access, as committee members, to the terms outlined—as MP Turnbull amended and as the Liberals voted for, ultimately—in the motion at our last meeting. Get the French quickly. It should not take some undefined period of time for the government to present it. We can't get on with the urgent nature of what we passed at the last meeting without, justifiably, a French version and an English version of the contracts.

I think the government should treat this with the most expediency and put all the resources it can into addressing the needs of this committee. I'm asking that they produce the translated documents very quickly. Once we get them, we'll pause for the day or two we need to look at the contracts. This isn't an indefinite pause. It's to give us the opportunity. Let's say we had them by Thursday. Instead of Thursday's meeting, we would have the day on Thursday to take a look at the contracts, if that's the way it works out.

Thank you, Mr. Chair.

The Chair: Procedurally, Mr. Perkins, I understand you're giving notice of the motion. You're not tabling it, because, if notice was not given, to table-drop a motion, it has to be on the topic discussed. We're on Bill C-27.

I understand there's one sentence at the end that would pause Bill C-27. It's not precisely on the topic. I'm tempted to say this cannot be discussed right now, because notice was not given, but I'll hear you out, Mr. Perkins, on that.

● (1715)

Mr. Rick Perkins: I appreciate that, but we are studying Bill C-27 now. That is the discussion we're having. We can ask any question we want of witnesses on Bill C-27, a very large bill. This is about the relationship of two studies and Bill C-27. I could point you to the procedures book—“the big green book”, as we all call it—and page 1061. The reference there allows us to reference the topic at hand that we're discussing. It would be in order.

Perhaps the clerk could take a look at that page. I know she knows this book inside out, because I've talked to her a lot about it in the past. She's very knowledgeable about it.

If you'd like, I could take a minute, or I could read it in. I don't think that's necessary, probably, since the clerk has it. It's on page 1061.

The Chair: I'll take a couple of minutes to read it myself, in order to determine whether this motion is receivable as a motion that has been table-dropped on the floor like this.

I'll briefly suspend. I apologize to the witnesses.

● (1715)

_____________________(Pause)_____________________

● (1720)

[*Translation*]

The Chair: Order, colleagues. We will resume the discussion.

[*English*]

We're on the motion that was just tabled by Mr. Perkins.

After considering Mr. Perkins' arguments and consulting with the clerk as well, I'll note that our routine motions—which the committee voted on at the beginning of this legislature and which were agreed on by all parties—state clearly, “That a 48-hour notice, interpreted as two nights, be required for any substantive motion to be moved in committee, unless the substantive motion relates directly to business then under consideration”.

I don't think the motion before the committee right now, which Mr. Perkins submitted, substantively deals with the matter at hand, which is Bill C-27. I understand, then, that this is notice given for this motion, and it will be receivable at our next committee meeting on Tuesday.

On that note, Mr. Perkins, you still have a minute for our witnesses. Otherwise, we can move to our next speaker.

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

Thank you, witnesses.

Mr. Goldfarb, I don't know if you're related to that famous Goldfarb pollster or not. You are. Okay. He was one of the innovators of polling in Canada. I don't know if he's your father, but he did great work.

I come at this as a marketing person when I look through this, and I know how much my colleagues—I won't say me—would push the envelope on analyzing data. This act is a brand new act—I'm talking about the privacy part—that would replace everything. The hole that's there in the buildup—as I mentioned to Dr. Guilmain—is from the “Purpose” section through to proposed section 15, “Consent”, and proposed subsection 18(3). I didn't mention proposed section 35, which allows the movement of data without a person's consent. It doesn't say it's limited to academic purposes, as PIPEDA does now.

Doesn't that actually create a big hole that marketers can exploit, combined with these weak consent provisions that are still there, and allow companies to still utilize your data, change the terms of reference, create new data uses without your permission and even—in the case of proposed subsection 18(3)—harm you? They can actually use it to harm you.

Does it not do that?

Prof. Avi Goldfarb: I'll be a little careful. I'm not a lawyer. I'm an economist. In my view, as an economist reading this, the harms of data flows are well protected, while at the same time, businesses and other organizations are going to be able to use data in ways that allow them to deliver better products and services to individuals—with the caveat of recognizing that I'm reading it with the eyes of an economist and not a legal scholar.

Mr. Rick Perkins: Proposed subsection 18(3) says that you can use it even if it harms the individual.

Perhaps I would ask that question of Dr. Guilmain, as well, as a lawyer. It's on the issue of proposed subsection 18(3) allowing for the data use even if it harms the individual. I'll give you a moment to take a look at it.

● (1725)

Mr. Antoine Guilmain: Would you mind repeating the question?

Mr. Rick Perkins: It reads, “the organization has a legitimate interest that outweighs any potential adverse effect on the individual resulting from that”. It's harm, basically.

Prof. Avi Goldfarb: Again, in my view, given my expertise as an economist, the explicit recognition of trade-offs is positive, and together with the explicit sentence that this is what somebody would expect if they were interacting with this company, it suggests a careful weighing of the trade-offs between the benefits of data flow and the benefits of privacy.

Mr. Rick Perkins: Thank you.

Maybe I can add one more caveat to that. I think the caveat that's always in here is “reasonable person”. The question is that there are a lot of people who aren't necessarily at that level in terms of their knowledge of the use of data. I think Europe actually may have a different standard that protects more vulnerable people than that term does.

Mr. Antoine Guilmain: Maybe I can give you a very simple example regarding cookies. We've all heard about cookies on websites, and 10 years ago cookies were very new, something that people didn't understand. Now, 10 years later—or more like 15 to 20 years later, actually—I think this is something that is well known by reasonable persons. Just to be clear, the fact that it's evolving is not bad. I think our laws are built on a notion like this, that essentially we are making things evolve.

What I see in proposed section 18, to be frank, is the assessment. The assessment makes me feel more comfortable in being able to say that this is rational and it's been explained. It's been detailed, and it's not just somebody saying, “You know what? I think I have a legitimate interest.”

Again, I understand that those are valid concerns. I hear you, but at the same time the world is changing fast. I think we can do tremendous work, and I think Bill C-27 is full of potential, but we need to accept as well that technology is going so fast that those kinds of concepts need to be embedded in the law.

That's my position.

Mr. Rick Perkins: Thank you very much.

The Chair: Monsieur Beauvais, I'll yield the floor to you because you've been patient.

Mr. Michael Beauvais: Thank you.

Mr. Perkins, I think any data protection laws are going to necessarily involve a weighing exercise. This is something that Mr. Goldfarb picked up on too. It's about weighing different interests.

I think that a lot of work could be done in proposed paragraph 18(4)(c) in terms of the prescribed requirements as part of the conditions of precedent, if there are specific concerns there. That's something that maybe the committee can think through quite carefully in terms of fixing specific things or addressing particular concerns regarding vulnerabilities of different users. I would also note that vulnerability is indeed a concept that appears throughout the GDPR, in particular its recitals.

Mr. Rick Perkins: Are you talking about adding definition to proposed paragraph 18(4)(c) through the act or through regulations?

Mr. Michael Beauvais: I mean that the concerns could be dealt with in terms of prescribed requirements issued by the minister instead of having them solidified into the legislation itself. I think it's unreasonable to say that absolutely no data used should possibly engender any sort of harm to any specific user. That would be treating privacy as an absolute. That, to me, as someone who consistently advocates for robust privacy protections, seems unreasonable.

[*Translation*]

The Chair: Thank you.

[*English*]

MP Van Bynen, the floor is yours.

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

My first question will go to Mr. Beauvais.

Do you feel that Bill C-27 gives the Privacy Commissioner of Canada enough tools to ensure that firms implement data management practices, considering the sensitive nature of personal information about minors?

Mr. Michael Beauvais: I would say that the bill specifically gives the Privacy Commissioner the ability to issue administrative monetary penalties, which is a very welcome addition.

The one thing that strikes me, which I would like to highlight, is the fact that at the moment the OPC cannot issue an AMP for breaches of proposed section 12. I think this is quite an important section, since the purposes of data processing are the pillar for determining what is or is not a legitimate use of data. Therefore, I would recommend including proposed section 12 as a kind of enforceable ground for the OPC.

● (1730)

Mr. Tony Van Bynen: Mr. Goldfarb, what are your thoughts?

Prof. Avi Goldfarb: I'm sorry, but what is the particular question?

Mr. Tony Van Bynen: Do you feel that Bill C-27 gives the minister and the Privacy Commissioner of Canada enough tools to ensure that firms implement data management practices, considering the sensitive nature of personal information?

Prof. Avi Goldfarb: I will be careful, a little bit, about my expertise in terms of the operations of it. That is not what I know well, but in my view, the bill is clear about what it gives the commissioner. If anything, I came in thinking that the commissioner is getting a lot of power out of this bill to potentially interfere with how small businesses and start-ups operate. I do think that, if anything, it does get the balance right.

Mr. Tony Van Bynen: Let's come back to an article that you coauthored and published in September, “The Economics of Digital Privacy”, in which you state that digital privacy regulations can “have negative consequences on market outcomes, particularly with respect to competition, innovation, and both producer and consumer surplus.”

Do you think that Bill C-27 should be amended to protect the competitiveness of Canadian businesses?

Prof. Avi Goldfarb: My view is that, in many ways, the most important thing about a policy—and, to some extent, a privacy policy—is to ensure that we protect competition.

At the same time, I don't know what an amendment to this act would look like in terms of protecting competition for the next generation of technology. A vigorous antitrust enforcement by the Competition Bureau and the continued vigilance on how large tech companies and others are potentially using their existing dominance in some markets to connect to and take advantage of new markets is worth protecting.

I'm not sure that belongs in Bill C-27, in the sense that things like ensuring interoperability between existing systems and new technologies are very valuable.

Mr. Tony Van Bynen: We're looking at some pretty significant imbalances in the economy where we have dominant players in relation to big data and financial resources.

What things should we be considering that level, or at least bring into better balance, the competitiveness of those imbalances now? The concern that I'm hearing through the HUMA committee is that this will be a polarization of capital and that the gap between the haves and the have-nots will become quite significant.

How can we address some balancing there?

Prof. Avi Goldfarb: When we think about technology and technological change, information technology is capital, so the owners of that capital have done better and better. This whole literature on the decreasing labour share and the increasing capital share of the economy is partly related to the ability to scale through information technology.

The impact of these particular data-driven technologies on market power is more subtle. The reason is that, in a Stats 101 sense—and I don't know if and when you took statistics—there are decreasing returns to scale and data in a formal technical sense. It's like this: If you have 10 people and you get an eleventh, you learn a lot; if you have a million people and you get one more, you don't learn that much. In an explicit technical sense, there are no economies of scale in data.

On data-driven and machine-learning technologies, there are reasons not to expect monopolization. There are, importantly, other forces going in the other direction, and those are the things that we should keep an eye on and regulate. The forces going in the other direction are things like.... The ability to use data requires certain other technologies or can benefit from certain other markets where there is dominance. The ability to use data, and use it well, requires computing, so if the cloud services market is monopolized or has strong market power, that's going to impede innovation and be a real competition worry. Also, if media, in some ways, are monopolized, and therefore the ability to understand users as they interact with media becomes monopolized, that's another way that could [*Technical difficulty—Editor*] in terms of competition.

In my view, those are related, but only tangentially related, to most of the content of Bill C-27.

● (1735)

The Chair: Mr. Van Bynen, I'm afraid you're out of time.

That concludes our third round of questioning, and we'll be ready to adjourn the meeting.

Mr. Masse, go ahead.

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

I don't get my last spot, and that's okay, but I want to say thank you. I appreciate your decision on the ruling. I think it's the right ruling in terms of the practice I've seen here.

I want to express my concern about the situation on the topic of jobs. When I came here on Monday, I was mocked by some members in the House of Commons because it was said that one job was going to be for workers from South Korea. We learned on Tuesday that it was 100 jobs. We learned today that there may be another 900 jobs that are possible—it's breaking right now. There was also the question of 1,600 jobs before that. We still don't know the jobs for building, tech transfer and operating.

I think those are all public trust issues that we should be getting to at some point. I appreciate your efforts to steer us through this. In my opinion, these are important investments to be made, but there needs to be some confidence and public trust, because it's not only about the plant that's local in my community, but the three that come after that.

I appreciate your ruling. I want to put on the record, though, that I think it was the appropriate reading given the practice, and the importance of the matter next week.

Thank you, Mr. Chair.

The Chair: We're not opening a debate. Mr. Masse agreed to forfeit his last two minutes of questions because we ran out of time, so I recognized him.

To be clear, I'm hoping that we're going to get the contracts very soon. I understand that they're being worked on by the department.

On that note, thank you very much to the witnesses for your presence here today.

[*Translation*]

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

The meeting is adjourned.

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

SPEAKER'S PERMISSION

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

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

PERMISSION DU PRÉSIDENT

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