



HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

44th PARLIAMENT, 1st SESSION

Standing Committee on Industry and Technology

EVIDENCE

NUMBER 093

Tuesday, October 31, 2023

Chair: Mr. Joël Lightbound



Standing Committee on Industry and Technology

Tuesday, October 31, 2023

• (1610)

[Translation]

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

Good afternoon, everyone.

Welcome to meeting No. 93 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 would like to welcome our many witnesses today and also apologize for the brief delay caused by votes in the house.

Today we welcome, from the Canadian Bankers Association, Lorraine Krugel, who is vice president, privacy and data.

From the Canadian Labour Congress, we have Siobhán Vipond, who is executive vice-president, and Chris Roberts, director, social and economic policy. From the Centre for Digital Rights, we have its founder, Jim Balsillie. From the Financial Data and Technology Association of North America, Steve Boms is with us via video conference.

From the Canadian Marketing Association, we have Sara Clodman, vice president, public affairs and thought leadership, and David Elder, head of privacy and data protection group, Stikeman Elliott LL. Lastly, we have, from the Canadian Chamber of Commerce, Catherine Fortin LeFaivre, who is vice president, strategic policy and global partnerships, and Ulrike Bahr-Gedalia, senior director, digital economy, technology and innovation.

So we have a lot of witnesses with us today. Once again, I thank you for being here.

I would also inform my member colleagues that the meeting will adjourn at 6:00 p.m. today. Please bear that in mind.

Without further ado, I give the floor to Ms. Krugel for five minutes.

[English]

Ms. Lorraine Krugel (Vice-President, Privacy and Data, Canadian Bankers Association): I would like to thank the committee for the opportunity to speak on Bill C-27, the consumer privacy protection act, or CPPA.

My name is Lorraine Krugel, and I am vice-president of privacy and data for the Canadian Bankers Association. The CBA is the voice of more than 60 banks operating in Canada, employing more than 280,000 Canadians and helping to drive Canada's economic growth and prosperity.

Banks have long been entrusted with significant amounts of personal information, and privacy and trust are paramount to our banks' customer relationships. As global data flows and technological advances have continued to increase, Canadian banks have been able to responsibly innovate to meet consumer demand for even more convenience, value and simplification. The CPPA reflects a unique, made-in-Canada approach that aims to address the needs of consumers and organizations in our evolving digital world.

We need to get this right. Some of the proposed provisions in the CPPA need to be better tailored for the Canadian context. We are concerned that there is a real risk of significant adverse consequences if the scope of certain provisions is not better defined and necessary exceptions are not included.

In particular, we would like to avoid situations where organizations would be required to provide too much information in order to be transparent. For example, certain transparency provisions could end up replicating the equivalent of consent fatigue or cookie banner fatigue, with no meaningful value to the consumer. Transparency obligations also require appropriate limits so that they cannot be abused or leveraged by criminals to circumvent processes designed to protect against fraud, money laundering or cyber-threats. In addition, we need to take care so that any requirements that are highly complex or operationally onerous would, in fact, address the right underlying risks and policy intent without negatively impacting legitimate operations, product and service delivery or the safeguarding of information.

The CBA is supportive of many of the key foundations of the CPPA. The CPPA is principles-based, scalable and technology-neutral and requires organizations to comply with a collection of interconnected provisions that provide a solid privacy foundation based on accountability, reasonability and proportionality; however, we see the need for targeted amendments in the following key areas: de-identification and anonymization, disposal requests and retention, and automated decision systems.

Relating to consent, we recommend an important technical amendment that will ensure continued alignment with provincial approaches while preserving policy intent and avoiding unintended consequences regarding consent obligations. In addition, we recommend an amendment to the CPPA to legally allow certain organizations to share personal information to combat money laundering and terrorist financing as part of a legislative framework that would be further defined through the Proceeds of Crime (Money Laundering) and Terrorist Financing Act. Done in the right way, such sharing could increase privacy protections for Canadians by reducing unnecessary reporting to the government on low-risk transactions and simultaneously increase the effectiveness of Canada's anti-money laundering regime through targeted and more effective reporting.

Finally, we believe that a minimum two-year implementation period is necessary to accommodate the scope of change and the development of regulations and guidance associated with the CPPA.

Regarding the artificial intelligence and data act, or AIDA, we are in the process of evaluating the minister's recent proposals and will be submitting comments and recommendations to the committee when the study focuses on the AI portions of the bill.

We have provided the committee with written comments and recommendations on the CPPA and look forward to your questions.

Thank you.

• (1615)

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

I'll now turn to the Canadian Labour Congress.

The floor is yours.

Ms. Siobhán Vipond (Executive Vice-President, Canadian Labour Congress): Good afternoon, committee members. It is my honour to be here with you today.

The 55 national and international unions affiliated with the Canadian Labour Congress bring together three million workers in virtually all sectors, industries, occupations and regions of the country. We are grateful for the opportunity to speak to the artificial intelligence and data act, AIDA, enacted by Bill C-27.

Across sectors, industries and occupations, workers in Canada increasingly encounter AI applications in their work and employment. Many report that AI has the potential to improve and enrich their work. In certain instances, AI applications could reduce time and energy spent on routine tasks. This could free workers up to focus on more skill-intensive aspects of their jobs, or on directly serving the public.

However, workers are also concerned about the negative potential consequences for jobs, privacy rights, discrimination and workplace surveillance. Workers are troubled by the potential for displacement and job loss from AI. Workers in creative industries and the performing arts are concerned about control over, and compensation for, their images and work. Workers are concerned about the collection, use and sharing of their personal data. Workers and unions are concerned about the use of AI in hiring, discipline and human resource management functions. Almost every week, we hear from workers who have real-life experience with the impact this is already having on their jobs. AI systems carry serious risks of racial discrimination, gender discrimination, and labour and human rights violations.

The number one demand from Canada's unions is greater transparency, consultation and information sharing around the introduction of AI systems in workplaces and Canadian society. Unfortunately, AIDA falls short in this respect.

Our concerns about AIDA are as follows.

First, unions are troubled by the lack of public debate and broad consultation on regulating AI in Canada. We feel there should have been proper public debate prior to the drafting and introduction of AIDA.

Second, the major deficiency of AIDA is that it exempts government and Crown corporations. The Government of Canada is a leading adopter and promoter of AI. Despite this, AIDA provides no protection for public service workers, whose work and employment are affected by AI systems. Government is responsible for many high-impact AI systems for decision-making—from immigration and benefits claims to policing and military operations. AIDA should be expressly expanded to apply to all federal departments, agencies and Crown corporations, including national security institutions.

Third, the bill only requires measures to prevent harms caused by high-impact systems. It leaves the definition of "high-impact systems" to regulation. As well, it is silent on AI systems that can cause real harms and discrimination despite falling outside the classification of "high-impact".

Fourth, AIDA contemplates a senior Innovation, Science and Economic Development Canada official acting as the AI and data commissioner. The commissioner should be an independent position. An office tasked with supervision and regulatory oversight should not be housed within the department responsible for promoting the AI industry.

Fifth, while AIDA authorizes the minister to establish an advisory committee, we strongly believe the government must go much further than the current advisory council on artificial intelligence, established in 2019. The advisory council is dominated by industry and academic voices, with no participation from civil society, human rights advocacy organizations, unions and the public. The CLC urges the government to create a permanent representative advisory council that makes recommendations on research needs, regulatory matters, and the administration and enforcement of AIDA.

Finally, the purpose clause of the act should be strengthened. Currently, AIDA is intended in part “to prohibit certain conduct in relation to artificial intelligence systems that may result in serious harm to individuals or harm to their interests.” This should be revised to prohibit conduct that may result in harm to individuals and groups, not just “serious harm”. Currently, AIDA is focused on individual harms, not on societal risks, such as to the environment or Canadian democracy.

In summary, the CLC believes there should be much more institutionalized transparency, information sharing and engagement around AI in the workplace and Canadian society.

Thank you. I welcome any questions the committee may have.

● (1620)

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

I'll now turn to Mr. Balsillie from the Centre for Digital Rights.

The floor is yours.

Mr. Jim Balsillie (Founder, Centre for Digital Rights): Chairman Lightbound and honourable members, thank you for the opportunity to share my views on Bill C-27, legislation that will have profound consequences on Canada's economic prosperity, freedom, democracy, consumer protection and child well-being.

The Digital Charter Implementation Act prioritizes the interests of large data monopolies and their ecosystem of traffickers. It sets a dangerous precedent by allowing corporations to allocate to individuals, children and vulnerable groups the harmful economic, political and social consequences of the data-driven economy. It normalizes and expands surveillance, treating human rights as an obstacle to corporate profits.

Bill C-27 requires a wholesale redo, and my written submission includes comprehensive proposed amendments.

A high-level perspective of some of the foundational flaws with the bill as tabled include the following: one, use of a notice and consent framework, which creates a pseudo-compliance system that enables personal data harvesting and intrusive profiling while spamming users with misleading consent barriers; two, a legitimate business interest carve-out that allows corporations to put the pursuit of profits above the interests of consumers, where businesses are allowed to privately self-determine what constitutes legitimate surveillance and behavioural modification to trample on fundamental rights but are under no obligation to notify consumers how they are tracking and profiling them; three, a diminishment of protections for children and vulnerable persons and an omission of meaningful measures that curtail insidious surveillance and behavioural manipulation practices that are driving the current youth mental

health crisis; and four, an artificial intelligence and data act that doesn't include an independent and expert regulator for automated decision systems and excludes the right to contest decisions made with AI, such as insurance, school admissions and credit scoring. AIDA needs to be scrapped completely.

There are many more flawed parts of this legislation, all detailed in my submission.

The recent letter by Minister Champagne indicating willingness to make some unspecified amendments is a woefully inadequate approach to dealing with the serious flaws in this bill. It joins the long list of bad governance practices, which is how we ended up with this untenable bill in the first place.

There has been much gaslighting from industry lobbyists and self-interested parties whose profits depend on mass surveillance, arguing that meaningful AI privacy regulations limit innovation. Privacy and AI regulations are not impediments to innovation. As innovation economists and digital policy experts have shown, the unique features of the data-driven economy—specifically, data's network effects alongside economies of scope, scale and information asymmetry—mean that the more data a company gathers, the more value it gains from it. Every new dataset makes all pre-existing datasets in the hands of the same few companies more valuable, disproportionately enhancing the power of established data giants and their vested assets. This is why, in less than a decade of the data-driven economy, we have seen the greatest market and wealth concentrations in economic history, a reduced rate of entrepreneurship, innovation and business dynamism and, also, lowered wages.

Properly regulating insidious data collection and trafficking, as other jurisdictions are doing, would not only address concentrated economic power, but also force business to compete on the level of quality and innovation, not surveillance and manipulation, as is currently the case.

I am an entrepreneur, investor, co-founder of the Council of Canadian Innovators, and a vocal advocate for Canadian technological and innovation success in global markets. It's deeply troubling to hear the government talk about advancing Canadian innovation, because earlier this year the government admitted that it has no AI strategy. We are merely funding basic research that principally supports the growth of foreign data monopolies.

This lack of capacity to understand and regulate the digital economy has real consequences, chief among them a steady decline in the standard of living and prosperity for the average Canadian, particularly in Ontario and Quebec, which used to drive our national prosperity. Because Canada is unable to create policies to harness the potential of IP, data and AI, the OECD recently projected that Canada's economy will be the worst-performing advanced economy of 2020-30 and the three decades thereafter.

● (1625)

The choice you have is to adopt Bill C-27, a deeply flawed attempt at privacy regulation, or to create new legislation that builds trust in the digital economy, supports Canadian prosperity and innovation and protects Canadians not only as consumers but as citizens. The choice is a continued erosion of Canadian prosperity, emboldening surveillance and manipulation and deepening the mental health crisis of our youth, or a healthy democracy, long-term prosperity, robust freedoms and the protection of our children.

Thank you.

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

We'll turn to the Financial Data and Technology Association of North America and Mr. Boms, who joins us online.

The floor is yours.

Mr. Steve Boms (Executive Director, Financial Data and Technology Association of North America): Thank you very much, Chair, and good afternoon.

I am the executive director of the Financial Data and Technology Association of North America, or FDATA. We're the leading trade association advocating for consumer-permissioned access to financial data in both Canada and the United States.

Our members include firms with a variety of different business models, which collectively provide more than six million Canadian consumers and SMEs with access to vital financial services and products. Utilizing these products, services and tools, Canadian consumers can, for example, access more competitive banking services, including more affordable credit. They could utilize more efficient payment options and benefit from technology to better manage their finances and grow their wealth. Canadian SMEs depend on FDATA North America member companies to manage their accounting and credit needs and more easily send and receive payments.

We are strong advocates of Canada's implementation of an open finance regime, which was first outlined as a government priority in budget 2018. The core idea of open finance is this: A Canadian consumer or SME should be able to safely and securely share access to their data held at one provider with another provider that offers a better financial product, service or tool. Whether it's a chequing, savings, business, brokerage, pension, mortgage, or auto loan account, or data held by a payroll or benefits provider, open finance is the straightforward notion that the customer should have the right to use that data for their own benefit.

Once built, open finance in Canada will put consumers and SMEs in full control of their financial data, facilitating a more transparent and competitive Canadian financial services market-

place that provides safe and secure data portability. The data portability right and data privacy framework included in Bill C-27 are fundamental cornerstones of this modernized approach to financial services.

A survey of Canadians commissioned last year by FDATA North America and Fintechs Canada found that half of Canadians feel stress when interacting with Canada's existing financial services sector and more than two-thirds of Canadians believe that more competition in the financial services marketplace would lead to a greater choice in products and lower financial services fees. Ninety per cent of Canadians indicated that they found fintech products easy to use, with more than 80% reporting they paid lower fees to fintechs than to their banks for similar services or products. Canadians deserve access to these alternatives.

Canada lags behind virtually every other G20 country with regard to open finance, data portability and data privacy. The U.K., Australia, New Zealand, Singapore, Brazil, the European Union and other jurisdictions have all enacted some version of government-led open finance, under which consumers and SMEs have legally binding data access rights and privacy protections afforded to them.

In contrast, today Canadian consumers and SMEs have no legal right to access or share access to their financial data. Unlike the overwhelming majority of other countries, in Canada, a consumer's or SME's bank is empowered to determine whether their customer may share elements of their data with a third party to get a better deal, access a new product or tool or avoid paying exorbitant fees. To the extent that a bank may allow its customers to do so, there are generally onerous and, in some cases, restrictive terms dictating the limitations under which their customers are able to do so.

While Canada has taken important steps towards such a regime since budget 2018, significant work remains to reach implementation.

Meanwhile, the rest of the world advances. Earlier this month, the United States formally launched its own open finance regime with a CFPB rule-making. Recognizing that incumbents in the financial services market will not, on their own, deliver a more competitive, customer-centric ecosystem, the director of the CFPB noted in his announcement that the rule will "supercharge competition, improve financial products and services, and discourage junk fees". Like Bill C-27, the CFPB rule would provide data portability rights to consumers and will require those firms that access—with their express consent—end-users' data to abide by strict data privacy and security provisions.

To advance its open finance regulations, the U.S. had an advantage that the Department of Finance and the Department of Innovation, Science and Economic Development currently do not: strong statutory authority to do so. Finance Canada has been studying how to deliver open finance in Canada for the better part of five years. FDATA views enactment of Bill C-27 as a critical element of the transition from open finance ideation to implementation. Once consumer and SME data portability has been enshrined in law, ISED and Finance Canada will have the statutory tools required to finally deliver open finance.

Consumers and SMEs in Canada are being left behind as the rest of the G20 build and deploy open finance frameworks that facilitate competition, enable greater access to and inclusion within the financial services marketplace and provide their citizens with appropriate data protections. The data portability and privacy provisions included in Bill C-27 represent integrally important statutory tools for ISED and Finance Canada that will help Canada catch up.

Thank you. I would be pleased to answer any questions.

• (1630)

The Chair: Thank you very much.

I'll now turn to the Canadian Marketing Association.

We have Ms. Clodman and Mr. Elder.

Ms. Sara Clodman (Vice-President, Public Affairs and Thought Leadership, Canadian Marketing Association): Good afternoon, Chair and members of the committee.

Thank you for inviting us to appear and for prioritizing privacy law reform. Your work is critically important to Canadians and to the future of our economy.

I cannot overstate how reliant Canadians are on data and the digital economy or how significant the proposed law is to Canada's future economic growth and to the protection of consumers.

The CPPA will enable small and medium-sized Canadian businesses to compete in the global marketplace. It will protect consumers through new consumer rights, greater transparency and accountability requirements for organizations, and the strongest financial penalties in the G7. It will help protect children. It will provide some support to the more than 80% of Canadians who are concerned about rising costs. It will foster innovation and allow Canadians to enjoy the enormous social and economic benefits of data.

The Canadian Marketing Association is the voice of the marketing profession. Our 450 members are small and medium-sized businesses, large brands, not-for-profits, and public and post-secondary institutions and organizations representing virtually all sectors of the economy.

We urge the speedy adoption of the CPPA. Consumers deserve modernized protections, and the businesses fuelling our economy need more regulatory certainty.

Consumer trust is critical to a successful business. Most organizations operating in Canada are responsible and are committed to building and maintaining a trusted relationship with their customers. They dedicate significant attention and resources to protect

personal information, including substantial investments in cybersecurity.

Canada's privacy law must protect consumers in a manner that does not create an unnecessary administrative burden for companies, including SMEs, which make up more than 90% of Canadian businesses. Canadian consumers expect organizations to intuitively deliver the products and services that they need and want. They are demanding faster and better, more relevant information from companies to help them make informed purchase decisions.

We are living in challenging economic times. Ninety per cent of consumers say that one of the most important reasons for sharing their data with companies is to receive discounts on products and services. With more than 80% of Canadians concerned about the rising cost of living, the personalization that comes from data usage provides some relief through relevant offers and sales that save them time and money.

To ensure that the CPPA meets its objectives while avoiding unintended consequences, we are proposing some limited amendments. Our first amendment calls for a more targeted and effective approach to protecting the personal information of minors. The CMA unequivocally supports the protection of minors. For decades, we have been the leader in setting standards for marketing to children and youth through the Canadian marketing code of ethics and standards.

We are concerned that the minors provision in the CPPA would result in an overcollection of data. Organizations that have no need to know whether their customers are minors should not be required to collect and retain people's birthdays, which is highly sensitive information, simply for the purpose of complying with the act. We propose that the provision for children in the CPPA be targeted to organizations whose business is directed to minors and to organizations that know or should know that they are processing the personal information of minors.

We also recommend that the law allow for different treatment of mature minors, who bear many of the responsibilities and enjoy many of the privileges of adulthood. These recommendations align with laws in the U.S. and Europe.

We have a handful of amendments in other areas, including consent provisions and the definition of ADS. We support the amendments by the Canadian Anonymization Network regarding de-identified and anonymized data, and we recommend a phased implementation period similar to that in Quebec. Our specific amendments are attached to our statement, and we are submitting a written brief outlining our views in more detail.

I'd like to close my remarks by emphasizing what this legislation is about and what it is not. The CPPA is intended to govern commercial activities. It would apply not only to large businesses and digital players, but also to very small organizations and to non-digital business activities. It would govern the ability of not-for-profits and charities to find and retain donors. The CPPA is not meant to address all aspects of the digital economy: for example, competition issues regarding data monopolies, the use of AI, which falls under AIDA, and protecting children from online harms. These are all critically important issues but do not fit within the scope of the CPPA.

• (1635)

Chair and members, our current law, PIPEDA, was the international gold standard for the protection of personal information for more than a decade. The CPPA builds on a strong legacy that Parliament can be proud of. Your speedy passage of this law can once again ensure that Canada leads the world in protecting privacy and fostering innovation.

I would like to thank the members of the committee for your leadership and service to Canadians.

Thank you.

[Translation]

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

I now give the floor to Ms. Fortin LeFaivre, who represents the Canadian Chamber of Commerce.

[English]

Ms. Catherine Fortin LeFaivre (Vice-President, Strategic Policy and Global Partnerships, Canadian Chamber of Commerce): Good afternoon.

I am pleased to appear before you on behalf of the Canadian Chamber of Commerce alongside my colleague, Ulrike Bahr-Gedalia.

[Translation]

The Canadian Chamber of Commerce represents more than 400 chambers of commerce and more than 200,000 businesses of all sizes, from coast to coast.

[English]

From the outset, we would like to state our support for modernizing privacy laws and for introducing guardrails regarding AI. We welcome the government's efforts to strengthen data protection for all Canadians, particularly children. CPPA must move forward to provide business certainty as soon as possible, while allowing for some amendments. There is concern about Canada's equivalency

with the EU, and the patchwork of provincial privacy legislation that is emerging in the interim.

Regarding AIDA, we believe that a more robust consultation process is required to properly address AI regulation needs in Canada. It's critical that our AI regulations are precise enough to provide important guardrails for safety, while allowing for our businesses to harness AI's full potential responsibly. This is especially relevant in the face of cross-sectoral skills shortages and SMEs that have dealt with one challenge after another.

[Translation]

Through Mr. Champagne's letter of October 20, we were pleased to hear that the government would address some major concerns related to the Artificial Intelligence and Data Act through their amendments, but we cannot substantially comment on these until they are made public and we've had time to consult with members.

[English]

Given the House Speaker's 2022 ruling that voting on parts 1 and 2 would be separate from part 3, AIDA, we urge the committee to contemplate how this avenue could allow for CPPA to move forward without delay, while making way for more in-depth consultations and input on the AI act to take place.

AI policy is indeed complex. Having the committee attempt to study privacy elements at the same time as quickly-changing AI elements doesn't provide the conditions for good policy to materialize. It's impossible to deny that AI regulations have become a global issue that's evolving rapidly. It's imperative that Canada not regulate in a vacuum. With major AI policy developments happening weekly, including the White House executive order on AI just yesterday, Canada must ensure we're taking steps to align our regulations accordingly. If not, organizations will have to contend with unique laws, making our country a less attractive destination for business.

I'll now turn it over to Ulrike.

Ms. Ulrike Bahr-Gedalia (Senior Director, Digital Economy, Technology and Innovation, Canadian Chamber of Commerce): Good afternoon, everyone.

Yes, indeed, we have received a long list of Bill C-27 recommendations from our members. A detailed brief was submitted to INDU in September and is available on the committee page, just so you're all aware. Please note that our analysis of the bill is ongoing as new material becomes available, such as the eight government amendments. Therefore, we are working with members to produce additional feedback to complement our earlier submission.

I'd like to take the opportunity to underscore a few key recommendations. First, a core position of the Canadian Chamber of Commerce is that there need to be amendments to better define many of the principles and concepts in Bill C-27 and to harmonize the bill with the norms and standards found in existing provincial and international law. Interoperability is paramount.

Among our recommendations on the CPPA, we are suggesting that the following elements align with Quebec's law 25: that the term "minor" be defined to include an age, that the definition of "anonymize" be in line with industry standards, and that the scope of the private right of action be narrowed. We also want to underscore the importance of legitimate interest exceptions in the current bill.

On AIDA, we were encouraged to see that government amendments would be forthcoming with respect to defining high-impact systems, creating clearer obligations along the AI value chain, and ensuring alignment with the EU AI act and those in other advanced economies. We look forward to seeing the text of these amendments to provide more specific feedback.

However, other matters remain unaddressed thus far, such as better defining the use of the term "harm". Our members have also raised serious concerns around the criminal liability element of AIDA, noting that Canada is the only jurisdiction in the world with such penalties. There is a belief that this provision might discourage businesses developing or deploying AI from setting up operations in Canada or even force some to leave, based on risk assessment.

Finally, in terms of coming into force, it's important that our businesses, especially SMEs—because small business is big business in Canada—have adequate time to adapt to new environments and requirements. We therefore recommend a phased implementation of CPPA and AIDA over a period of 36 months.

Thank you very much.

• (1640)

[Translation]

The Chair: Thank you very much.

We will immediately begin the discussion.

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

[English]

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

Thank you, witnesses. I know the tremendous amount of work you've all done in preparing to be here today, and I want to thank you for the amount of time you've spent with me over the last number of months to expand and have a two-way conversation on how we can improve this bill. It's really three bills and a complete replacement of the Privacy Act, which is why it's so comprehensive and huge for us to deal with. If we passed the artificial intelligence bill, we'd probably be the first country in the world to actually get one passed, because one hasn't really been passed yet that I'm aware of.

Maybe I can start, because I have limited time.

Mr. Balsillie, as the co-founder of one of Canada's most iconic companies, BlackBerry, which we were all addicted to at one time—I wish I still were—you have some expertise on the idea of innovation and what it takes to do innovation while balancing that with protecting people's privacy. This new Liberal bill, which is on the privacy side, is a bit of a rehash of a bill from the last Parliament, which didn't make it through. In my view, it puts the interests of corporations ahead of those of the individuals and the protection of their privacy, since the purpose section, which is proposed section 5, says that the protection of personal privacy and the fundamental right of businesses to access that information are of equal importance. A subsequent series of clauses actually give businesses more say, including proposed section 18 on legitimate interest and the exceptions to express consent.

Do you agree that it's putting the interests of large corporations and corporations in general ahead of individual privacy rights?

Mr. Jim Balsillie: Thank you for that question.

A fundamental right should be inalienable, not balanced. In Europe, where you have the ability...it's the very narrowest of special circumstances, but this idea that it's some kind of balanced proportionality does not make it fundamental and does not make it inalienable. It's a fundamental flaw in the approach to it. It's either an important right or it's not.

• (1645)

Mr. Rick Perkins: So, you would suggest, then, that if fundamental right is put into proposed section 5 of the CPPA, as we proposed—I think as the NDP had, and now as the minister acknowledges needs to be done—it should have some sort of legal wording that gives that paramountcy over the corporation's right in that clause.

Mr. Jim Balsillie: That's correct. Absolutely.

Mr. Rick Perkins: In hearing witnesses so far... We have a lot more to hear, and we wish we could have more time than we do. However, a number have said that we have to be very careful in finding the fine line and the balance between protecting individual privacy and squashing innovation and driving business out of Canada if we go too overboard on protecting an individual's privacy. Do you agree that that's a concern in protecting individual privacy?

Mr. Jim Balsillie: Not at all.

I have a bit of an advantage over everyone here in that I was in the small meeting where then Minister Bains and then deputy minister Knubley presented the original Bill C-11. They said that they were approaching this as some kind of balance, and I said, "Who concocted this concept of a trade-off between the two?" They, in fact, re-enforce each other. It's a false dichotomy.

Mr. Rick Perkins: One of the ways they do that—and I actually don't think it's a balance; it's slanted towards businesses—is in proposed subsection 15(5) of the CPPA, which is the consent section. The bill actually allows for implied consent and allows a business to say, “Well, I think you agreed to this, so I'll decide to use your data.”

Proposed subsection 18(3) says that if a business's “legitimate interest” is more important than the individual's, then the corporation can use the data as it wishes—in fact, even if it harms people.

Proposed section 35 takes out the old language about scholarly studies that says that research can be done for scholarly studies. Proposed section 35 gives organizations the right to collect and use data however they wish.

To me, it seems pretty wide open. Would you agree that those specific clauses should be deleted from the bill?

Mr. Jim Balsillie: Absolutely.

Mr. Rick Perkins: Okay.

One of the issues that have been raised quite a bit is this issue of collective group rights. As a marketer, I knew that I could buy databases from across the world, try to de-identify stuff, and try to target certain people because of certain behaviours. Do you believe that this bill does anything to deal with the issue of corporations trying to use group data to infer certain behaviours?

Mr. Jim Balsillie: No, it doesn't—and it should, because when you make a decision, you affect those around you, who are affected by the nature of the digital footprint that we collectively leave. Also, if you opt out but are part of a group that has agreed to these things, you are profiled in that, even though you have pulled yourself out of it.

Understanding both the individual effects and the collective effects needs to be a central aspect of this bill.

Mr. Rick Perkins: The Centre for Digital Rights' presentation to the committee talked about cross-border flows of data. We know that this is what businesses of all sizes do now and that other jurisdictions have looked at this issue of cross-border flows of data, but this bill is silent on cross-border data flows.

Can you outline the inherent dangers to the protection of privacy without any framework around cross-border flows? What do you think should be included in there?

Mr. Jim Balsillie: Sure.

That's the root of the contention between the EU and the U.S.—that you must have a sufficiency realm that the data is going to that maintains the European threshold or else they don't allow the data to be transferred. That's been the tremendous contention of the Europeans in standing up for European citizens.

If you have these rules here but they can move to another jurisdiction that has lower standards, then all of those protections are stripped. If it's boomeranging across, going from coast to coast in Canada, but it boomerangs through a node in the U.S., it's all stripped.

Mr. Rick Perkins: Thank you.

The Chair: Thank you very much.

Mr. Sorbara, go ahead.

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

Welcome, everyone.

Bill C-27 is a very important bill for consumers, for individuals and for businesses, both domestically and internationally. One of the things I've been able to glean just from the testimony today is the regulatory alignment that's needed between us and other jurisdictions, and also that we in Canada benefit, sometimes, from what's called a fiscal federation. Sometimes the provinces move first, and sometimes we do, but we need to be on the same page due to the importance of the material here.

This is for the Canadian Bankers Association.

In 2018, I was part of the finance committee when we did the statutory review on money laundering and terrorist financing. “Moving Canada Forward” was a report that we issued in November 2018. You've raised some good things and some potential amendments and so forth with regard to the CPPA in relation to money laundering and terrorist financing. Can you comment on that and add any more colour that you wish to add in that vein?

• (1650)

Ms. Lorraine Krugel: Thank you for the question.

With the money-laundering piece, certainly when we look at other jurisdictions, Canada is behind with respect to combatting money laundering and terrorist financing. Other case studies are already in play in Europe, Estonia, Netherlands and the U.K. There is also information sharing in the U.S. This allows those organizations to uncover networks of criminal organizations that are leveraging the fact that individual organizations in Canada have to report to the government, but they cannot follow up to see whether or not the transactions will go to another organization. That other organization may not be reporting to the government, so the government cannot see the whole piece of the puzzle with respect to those criminal networks.

This information sharing will allow for more targeted and effective reporting. We believe that it will actually increase the privacy of Canadians. Right now, when we look at the amount of reporting that goes from organizations to the government on a per capita basis, it's twelve and a half times more than in the U.S. and 96 times more than in the U.K.

The approach we're proposing is narrower than what the GDPR permits. Many organizations can leverage the legitimate interest provision in Europe to be able to do this type of sharing. Because the legitimate interest in the CPPA does not permit disclosures, we're proposing that it be linked to the proceeds of crime act to really limit that sharing.

Mr. Francesco Sorbara: Okay.

I would like to follow up. I believe the CMA commented that it enabled small and medium-sized businesses to compete in the global economy through Bill C-27 as it is. Can you elaborate on that? Bill C-27 is a pretty in-depth bill. I almost wish I had gone to law school to understand most of it, but we're trying to get through it. Could you comment on that aspect quickly?

Then I have a follow-up question for Mr. Balsillie, if I have time.

Ms. Sara Clodman: Thank you for the question.

The law is designed to be principles-based. It does take into account the size and type of business and the activities that an organization is engaged in. It is very different from the European law, which is very prescriptive, requires pages of box-ticking and needs privacy lawyers to help people even understand. Even privacy lawyers there have trouble understanding the requirements. For small businesses here, that would be impossible.

This bill is much more balanced.

Mr. Francesco Sorbara: Mr. Balsillie, I had the pleasure of sitting with you when Mr. Breton, the European commissioner, was here. I believe it was last year or something like that. I think we were talking somewhat about the issues that we're talking about today.

The Europeans have been the first movers on a lot of aspects of the new economy or industrial revolution 4.0 or 5.0—whichever clichéd term we want to use. You have brought your views here in terms of what you think is wrong and why. I respect that, of course. We all do.

In terms of what Bill C-27 intends to do in relation to the modernization of privacy and how we deal with privacy and AI, are there aspects of the bill where we are going in the right direction? Is it just absolutely going in the completely wrong direction?

Mr. Jim Balsillie: It's like saying that my bucket has 25 holes in it and that's better than 30 holes, or if we get rid of 20 of the holes, then we'll only have 10 left. I think the nature of the digital economy and the knowledge economy is that it's non-linear in its harms from imperfection. It takes a small hole to drive a truck through, so you need relative completeness or somebody will escape through a small hatch.

• (1655)

Mr. Francesco Sorbara: I will say that if we're getting rid of 20 of the 25 holes, I think we're making progress.

Mr. Jim Balsillie: But you still have five holes in your bucket, so it's not a bucket. That's my point.

The point is that incompleteness is deeply harmful, with the nature of the knowledge economy and the data economy. That's why Canada is faltering with these prosperity and citizen wellness effects. We have to be complete.

[*Translation*]

The Chair: Thank you, Mr. Sorbara.

Mr. Villemure, the floor is yours.

Mr. René Villemure (Trois-Rivières, BQ): Thank you very much, Mr. Chair.

Ms. Vipond, if memory serves me, I believe you testified before the Standing Committee on Access to Information, Privacy and Ethics not long ago.

The minister discussed a voluntary code of conduct regarding the self-regulation of artificial intelligence. Do you think that's a realistic proposal?

[*English*]

Mr. Chris Roberts (Director, Social and Economic Policy, Canadian Labour Congress): Can you repeat the question?

Ms. Siobhán Vipond: Yes. I'm sorry. Can you repeat it?

[*Translation*]

Mr. René Villemure (Trois-Rivières, BQ): Yes.

Mr. Champagne proposed a voluntary code of conduct for businesses that would involve self-regulation. I'd like to know if you think that's a realistic proposal.

[*English*]

Ms. Siobhán Vipond: Thank you for the question. My apologies for making you repeat it.

I think that any time we go into voluntary we get into trouble, just as a fundamental approach to the work, so we do have major concerns there.

I would like to pass it on to my colleague, Chris, to flesh out our response on that.

Mr. Chris Roberts: It's just that: I think industry self-regulation in such an important area is precisely not what we need at the moment. We need clear statutory and regulatory rules around industry and clear expectations from industry.

[*Translation*]

Mr. René Villemure: Thank you very much.

Mr. Balsillie, what do you think the foreseeable effects of Bill C-27 will be based on jurisdictions and, in particular, in comparison to Quebec's Bill 25?

[*English*]

Mr. Jim Balsillie: To contrast it with bill 25 in Quebec and its effect on Quebec, I think the strategic approach of Bill C-27 will disproportionately harm Quebec, worse than any other region in Canada, for several reasons.

Number one, when you commodify social relationships and cultural properties and they can be exfiltrated and exploited, then you diminish the distinct social society in its control within the province.

Second, when you create ambiguities or different thresholds between the federal and the provincial, you'll naturally have lawyers go deeply into exploiting the lower threshold. You're seeing that happen with federal-provincial party data, where they're saying that the feds control federal political data even though law 25 says that's a provincial realm, but the position of the lawyers, in a judicial review happening in British Columbia now, is that it is not true.

Third, businesses will naturally arbitrage to the lowest jurisdiction. Picture a river between Quebec and another province. If there's a high environmental rule on the Quebec side of the river and a lower on the other side, the business will go to the lower part, even though it's all the same river.

The best way to protect Quebec, Quebec society and the Quebec economy is to make sure that every aspect of this bill is equal or superior to the principles that are in law 25, and currently that is not the case.

[Translation]

Mr. René Villemure: In a report from last year, you discussed a concern about surveillance in connection with Bill C-27.

Would you please clarify the concept of surveillance? What were your fears?

[English]

Mr. Jim Balsillie: Well, the nature of the contemporary economy, the data economy, is that you absorb data on people to manipulate them, and you use that data to do all kinds of things that benefit the keeper, the controller, of that data, who puts them into algorithms.

My view of this is that you need to deal with this *ex ante*. Who says you can collect that data? Who says you're allowed to manipulate me? I come here representing civil society, as a citizen. The harms of mismanagement here are deep and they are great, and they don't benefit Canada or Canadians in this model.

When I was young, teachers smoked cigarettes in the classroom. We are going to look back 10 years from now and say that it was remarkably absurd that we did this to our children and our society. This is your chance to be on the right side of history: what is good for society, the vulnerable and the country, and what is not.

• (1700)

[Translation]

Mr. René Villemure: Do you think the bill will enable end users to understand how their data and consent will ultimately be used? Do you think users will be able to understand what they're consenting to?

[English]

Mr. Jim Balsillie: The answer is no, because so many of the people who consent are forced into a consent model or there's implied consent or there's no need to disclose there is consent. There are aspects of algorithms that who knows if you can contest if you don't know what's going on.

Look at the mental health crisis for our kids. What is driving this? What does that say about our society? This is a product of ma-

nipulation of vulnerable people, whether it's older people, younger people or marginalized people.

[Translation]

Mr. René Villemure: So it's manipulation in every case.

[English]

Mr. Jim Balsillie: Yes.

[Translation]

Mr. René Villemure: You said the government didn't have a strategy in the matter. Could you tell us more about that?

[English]

Mr. Jim Balsillie: Yes. I went to the government when they said they had the first national AI strategy, and they said there were no documents. That was reported in the news—in *The Globe and Mail*—in February.

[Translation]

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

I now yield the floor to Ms. McPherson.

[English]

Ms. Heather McPherson (Edmonton Strathcona, NDP): Thank you, Mr. Chair, and thank you for letting me join you at this committee today.

I have some questions for our guests from the Canadian Labour Congress, if I could.

First of all, there have been concerns raised about the risks and limitations of housing the AI and data commissioner in ISED. Could you elaborate on the problems and concerns of this model? Could you also perhaps comment on whether or not it would be more effective, transparent and accountable if the AI and data commissioner was completely independent and was an officer of Parliament, like the Parliamentary Budget Officer?

Thank you.

Ms. Siobhán Vipond: As we stated, currently, by housing it in the same place, we're asking for the promotion of AI to happen but also for the checks and balances to supposedly happen in the same place. We know that independence would offer an opportunity to ensure that we're meeting what should be the goals: What is the effect on Canadians? What is the effect on democracy?

It's not reasonable to expect that those whose job is actually to promote AI are able to put those checks and balances in place as well. We believe it absolutely should be housed separately.

Ms. Heather McPherson: Thank you very much, Ms. Vipond.

It's nice to see you, by the way. I wish I were there to see you in person.

My next question is this. Since this bill was introduced, as it has progressed over the year it's been in the House, many issues have been raised about the consultations that have taken place. Specifically, concerns have been raised about the limits of the existing AI advisory council as a way to engage civil society on AI.

Could you elaborate on these limits and on what you would suggest would be a better model?

Ms. Siobhán Vipond: Absolutely. We are strong believers that social dialogue is our best position to make any decision. Getting to this point, where there hasn't been enough social dialogue—especially, for us, involving unions as part of that.... We have big concerns. What are we trying to protect?

Workers are excited about certain parts of AI, but they're also very concerned. The wrong type of design will send us down a road that could have huge impacts on people's jobs. Currently, we're not part of that dialogue in a way in which we can actually make sure that this is designed so that we are ensuring that this is an opportunity and that we are mitigating the risk to jobs and to workers.

Ms. Heather McPherson: Thank you.

As the evaluation and analysis of this bill have progressed, questions about why we think government and Crown corporations should be included in the scope of the act have been raised. Perhaps you could just provide some of your thoughts on this and why you think, or possibly believe, that the government and Crown corporations should be included.

• (1705)

Ms. Siobhán Vipond: Absolutely. From a workers' point of view, by excluding Crown corporations and government, we've excluded a significant number of workers who are affected by AI. In a lot of good ways, Crown corporations and our government have invested in AI and are developing AI, but they are somehow not going to be part of the regulations or rules around that, or be part of the discussions we're having, and should be having, around this bill.

We strongly support all those workers who need to be included so that we can see that we are keeping checks and balances and there are mandatory rules and regulations around what's being done in terms of workplaces within the Crown corporations and the government.

Ms. Heather McPherson: Thank you.

From your perspective, I'd like a little bit of insight on how AI regulation has been approached in Canada versus the United States, and which mechanisms and which things you prefer.

Ms. Siobhán Vipond: I think we're all aware of the executive order that came down yesterday. I think the beginning of that executive order from President Biden starts with the need to look at how Americans are affected. I think that's what we should be doing here in Canada. How are people being affected? That is the starting point. How are workers being affected?

Then, when you look further in terms of what the executive order in the United States is stating, it's also recognizing the impact on workers, the impact on unions and the role that unions should play in that discussion in terms of designing it. It's also laying out that there needs to be constant evaluation, whether it's around the im-

pact on jobs or the impact on equity, which is all work that we believe should continue.

As we said at the beginning, we can design this so that we're having discussions and putting ourselves in a position of opportunity, or we can design this in a way where we're undermining the work that I think we need to be doing further. For us, there's not enough balance in terms of approaching this. It has to be about people. It has to be about workers. We have to ensure that workers are part of that discussion and respect the commitment we have in Canada to social dialogue.

Ms. Heather McPherson: Thank you.

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

The Chair: You're over by five seconds, Ms. McPherson, but we'll get back to you.

I will now yield the floor to Mr. Vis, for five minutes.

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

I'm going to start with the Canadian Marketing Association.

Ms. Clodman, would you be comfortable collecting and using sensitive information of minors for a socially beneficial purpose, as defined in the legislation, without the proposed legislation defining what a minor is?

Ms. Sara Clodman: The Canadian Marketing Association has been a leader in developing rules and guidance for marketers when it comes to using children's information. We have rules that start at anyone under 13, and any use of their data would need the express consent of the parent.

Mr. Brad Vis: How can a parent provide express consent for a child's information when that child might just simply agree to provide consent on a computer application without the parent's knowledge? How would a company differentiate between data collected in an inappropriate way, or in certain cases, as you mentioned, when the parent did provide that consent?

Ms. Sara Clodman: In the case of children, our view is that if it's a company that is dealing in an area where it knows it is specifically reaching children, it should set up a system to make sure it is getting the parental consent.

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

Would you agree that we might consider looking at the U.K. model, which has tiered ages of consent? In fact, it has five different levels related to minors, indicating how information is collected in each of those circumstances.

You mentioned that 13 is a threshold age. Can we do a better job in Canada by including in this legislation a specific and detailed protocol that ensures children are not exploited online for commercial purposes?

Ms. Sara Clodman: If you're talking about an online harms type of thing, that would be different legislation.

This bill deals with privacy.

Mr. Brad Vis: No, I am talking about commercial or business interests.

Ms. Sara Clodman: In terms of privacy, our code actually does have three steps, not five.

Mr. Brad Vis: For this legislation, though, and not your code, do you believe we should enshrine very prescriptive language in this legislation to protect children?

• (1710)

Ms. Sara Clodman: That is something I'd have to take back to my membership in terms of how detailed it should be in the legislation.

Mr. Brad Vis: Thank you for your time.

Mr. Balsillie, first off, thank you for your comments. I really do feel... I am very concerned about this bill. I think it is broken, primarily because the minister came before our committee and said that he wanted to protect children but didn't define in the legislation what a fundamental right to privacy would be for a child, even though it's a second iteration of this bill itself. That's very problematic for me.

On page three of your report, "Not Fit For Purpose—Canada Deserves Much Better", regarding this bill, it states, "Most importantly, it fails to address the reality that dominant data-driven enterprises have shifted away from a service-oriented business model towards one that relies on monetizing PI".

I am so concerned about the mental health crisis you outlined with respect to youth and the vulnerability that children face every day when they go online, even in their own classroom, as was outlined in a Globe and Mail report last year.

Is there any circumstance...? Are we getting to the point that we need to put the hammer down as legislators and go really far in protecting children in this bill, because we have no idea what harms are going to come their way in the next 10-15 years?

Mr. Jim Balsillie: I welcome your question.

Not to drop names, but I keep very close relationships with good friends on this, like Beeban Kidron, who is founder and chair of the U.K. 5Rights Foundation for kids, and Shoshana Zuboff, with whom I am very close and we'll be here together in Ottawa in February with many other developmental psychologists.

Fundamentally, when we were growing up, when something happened to you, you went into your bedroom and you licked your wounds for a couple of hours or a day, and you came back out. In this current process, where you cannot retreat and heal, there is a permanent record of this, and it undermines the healthy developmental process.

I could go on and on.

Mr. Brad Vis: [*Inaudible—Editor*]

The Chair: Mr. Vis, I'm sorry. Your time's up, and there's something wrong with your microphone. Out of courtesy to the interpreters, we'll stop it there.

I'll now turn to Madame Lapointe.

[*Translation*]

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

[*English*]

My first question is for Ms. Krugel.

Some stakeholders have raised concerns about the fine balance we need in order to ensure that the privacy of Canadians is fully protected through this legislation, while also allowing for the positive benefits of online tools that use data to drive innovation. What is your perspective on how we can find that appropriate balance?

Ms. Lorraine Krugel: We believe that PIPEDA actually had a lot of elements around this. It already had organizations considering what was reasonable and what would be reasonable uses relating to personal information. That was in the Privacy Commissioner's guidance a lot. Now we see the CPPA taking those good things from PIPEDA and encoding the Privacy Commissioner's guidance around appropriate uses and reasonability.

When it comes to innovation, we believe there is a need for organizations to be able to leverage the information in a responsible way to be able to do this. We see this in some of the areas where there's more permission to use de-identified information for internal research and development and analytics purposes—again, in a responsible way.

We want to make sure that there are appropriate limits on some of this as well. We have a concern with respect to the prohibition on reidentifying information, because we believe that a lot of organizations, when they do their analysis and are looking for ways to innovate, will often de-identify information just to keep it safe. When you have a prohibition on reidentifying it, organizations won't do de-identification just for safeguarding. We think that's one area where an improvement can be made, but the use of de-identified information for internal purposes is very welcome.

Ms. Viviane Lapointe: Thank you.

My next question is for Ms. Clodman.

You mentioned in the opening statement that your organization serves many small and medium-sized enterprises. Can you tell this committee what the key considerations for SMEs would be in privacy law? In your view, does the consumer privacy protection act reflect these considerations?

• (1715)

Ms. Sara Clodman: I think the most important thing is take into account the variable capabilities of SMEs when they are collecting data, and I think the bill does achieve that. It needs a few tweaks in order to really help SMEs.

One of the most significant ones would be in the area of children's data. Careful consideration has to be made when thinking about what the rules should be. The simple provision that's in the bill right now is a very blunt instrument to deal with a very important topic.

For example, if a child goes to Canadian Tire to buy a mug, or if any person goes to Canadian Tire to buy a mug, with this provision, in the way it's written, Canadian Tire will have to determine whether that person is a minor. If so, the data will have to be bucketed separately. It's day-to-day transactions like that, not just for large organizations, but for small organizations. They would have to be able to keep track of which of their customers are minors. When they're not selling products to minors, or absent things where there are concerns, it's a lot of extra administrative work that is very costly for small businesses.

Ms. Viviane Lapointe: Can you tell us how the exceptions to consent in the consumer privacy protection act compare to the European Union's privacy laws?

Ms. Sara Clodman: Let me start by saying that consent and informed consent are extremely important in any privacy law. Those rules exist as well. The CPPA calls for clearer disclosure built on the existing rules, but the Achilles heel of disclosure is consent fatigue. In Europe, people have to consent to so much all the time that they don't carefully read the notices about what they're consenting to, so their consent becomes less well informed.

That is a major issue and it's something we'd like to avoid here.

[Translation]

The Chair: Thank you, Ms. Lapointe.

You have the floor, Mr. Villemure.

Mr. René Villemure: Thank you very much, Mr. Chair.

Ms. Vipond, there are a lot of creators in my riding of Trois-Rivières.

Do you think that the part of the bill concerning artificial intelligence protects creators?

[English]

Ms. Siobhán Vipond: Thank you for the question.

This is a big concern that folks who work in the creative industries have, because, again, it's about the discussion. What does a compensation model look like? We're hearing that a lot in the media right now around performers and how their image can be looked at and used past the point.... Are they being compensated properly?

We also hear about creation, whether it's writing or the creation of art, and what happens to that afterwards. I don't think it's being addressed in an appropriate way, but we also aren't setting the table for those workers to be at the table to actually have those discussions so that we can be building it in the right way.

[Translation]

Mr. René Villemure: Thank you very much.

Mr. Balsillie, do you think this bill protects creators?

[English]

Mr. Jim Balsillie: No, I do not. I think the mistake with the creators, particularly in relation to Ms. Vipond's comment on AI, is that the government put its shoes on first and is now trying to put on its socks, and we have to start over.

You begin with the consultation and the dialogue with the stakeholders. Then you create your white paper, and then you go to legislation. Now we're trying to figure out what to do with our socks without taking off our shoes. We just have to take them off and start over.

[Translation]

Mr. René Villemure: Creators in my riding are very concerned and feel powerless.

What could we do to improve the bill and reassure creators?

[English]

Mr. Jim Balsillie: We have to understand that we live in a world of digital mediation that has economic and non-economic effects, but how we govern these is through social structures.

When the car was invented, we decided there should be speed limits in front of schools and blood alcohol limits. It's the same here. In economics, you begin with norms. You define what you value, and then you work back from there with an appropriate tool kit. We do have the tool kits to achieve our norms, but we have to put our norms up front, and then we have to be cognizant of what's an effective tool kit to manifest it.

I think you have all the power in the world to create historic legislation here. I just want to see that you actually manifest the norms that you care about.

• (1720)

[Translation]

Mr. René Villemure: As an ethicist, I am very happy to hear you refer to norms and values that must be in harmony in order to create this act, which would be exemplary.

You've previously spoken out about the fact that political parties aren't subject to Bill C-27. Would you please clarify that view a little further?

[English]

Mr. Jim Balsillie: Yes, in Europe, for adequacy—and don't assume this bill will get adequacy in Europe—the two most sensitive types of information are children's information and political party information, which were not included in Bill C-27.

There's a minimum standard in British Columbia, and the political parties under the budget bill are claiming that they trump that under a judicial review right now, which is effectively no oversight whatsoever. It shows that you're playing with our democratic structures, our global adequacy and what is a constitutional realm for the provinces and the federal level here. I don't know for what purpose. I don't see anything wrong with raising an appropriate standard and then putting together the proper tool kit to look after the country we all love.

[Translation]

Mr. René Villemure: You mentioned Shoshana Zuboff earlier. Do you think that Bill C-27 will encourage or stifle surveillance capitalism?

[English]

Mr. Jim Balsillie: Bill C-27 turbocharges surveillance capitalism. I talked to Shoshana last week, and we worked through this. She is coming here in February. This turbocharge is insane.

[Translation]

Mr. René Villemure: That's very interesting. Thank you.

Ms. Fortin LeFaivre, do you think that Bill C-27 should align with Quebec's legislation and that the latter should prevail?

Ms. Catherine Fortin LeFaivre: From what our members have told us, certain specific elements should be aligned with Quebec's Bill 25. I'm thinking of the word “minor”, for example. The age is set at 14 in Quebec. We think we should rely on that. I'm also thinking of the definition of “anonymize” and of the scope of the individual right of recourse. Several elements rely on the principle of interoperability.

Many businesses already comply with Bill 25, which was passed last year, and tell us we should adopt certain aspects of that legislation.

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

Go ahead, Ms. McPherson.

[English]

Ms. Heather McPherson: Thank you very much, Mr. Chair.

Mr. Balsillie, I have a question for you about the privacy tribunal—similar to the Competition Tribunal that exists—where decisions, rulings or potential orders of the Privacy Commissioner would be challenged by organizations or businesses. This has been demonstrated by the Competition Bureau's rejecting and reversing decisions of the competition commissioner in the case of Rogers' takeover of Shaw, for example.

Other countries do not have this additional quasi-judicial body that seems to obstruct what independent agencies have decided. Parties to these decisions of the Privacy Commissioner can always go to the Federal Court, as in other countries, if they disagree with the decision. In fact, they can go to the Federal Court even to appeal the decisions of the privacy tribunal.

What is your opinion of the privacy tribunal? Is this an extra layer that just delays function and will hinder the Privacy Commissioner's office from carrying out its necessary functions and enforcing its decisions?

Mr. Jim Balsillie: I don't know who came up with this idea of a tribunal. I think it's a mistake; it shouldn't be there. It undermines the courts. It undermines the commissioner. I think it just adds another layer, as you said. If you're a corporation trying to negotiate with the commissioner, you'll just shrug your shoulders and say, “I'll see you in the tribunal”, which is quasi-judicial.

Why do we need it when we have perfectly legitimate courts that are bound by all the jurisprudence? No other country in the world

has it. Nobody asked for it. Who in the world inserted this and under what kind of consultation? When I saw it, I thought, “Who did this?”

Ms. Heather McPherson: That's very clear. Thank you, Mr. Balsillie.

Ms. Vipond, could you provide your perspective on that as well, please?

Ms. Siobhán Vipond: Yes. For us, there has to be an ability for checks and balances. As we've said before, it needs to exist outside of that process.

Then, overall, when we're just looking at who has a say in the decision-making, we're always going to go back to that. We're not there yet. We need to have more social dialogue before we get to the point of looking past that point.

• (1725)

Ms. Heather McPherson: Thank you.

I'll just stick with you for one last question very quickly.

Why should directors and officers be held personally liable for violations of their businesses?

Ms. Siobhán Vipond: It's because people make decisions, and those decisions have impacts. This idea that you are suddenly not responsible for what happens alleviates a chain of responsibility that needs to exist. We see this when we're looking at almost all labour law, where, if you make decisions in a workplace, that has an effect. If you make decisions that are going to have an effect, you should be liable or you should be responsible for those decisions. That's why we're advocating for that.

Ms. Heather McPherson: Thank you very much.

[Translation]

The Chair: Thank you very much.

Mr. Généreux, you have the floor.

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

Thanks to the witnesses. Welcome to the great Liberal darkness club. This makes me feel like a dog chasing its tail. I use that metaphor because I just saw Ms. McPherson's dog on the screen.

We are all here to discuss a bill that, as Mr. Champagne announced to us three weeks ago, would be subject to eight amendments, some of which will be major.

Mr. Balsillie, earlier you said that Mr. Bains consulted you at the time about Bill C-11 and that you had made recommendations. The current minister, Mr. Champagne, tells us he has consulted 300 organizations and experts.

Ms. Vipond, you clearly weren't in the group. At any rate, many of the witnesses here probably weren't in the consulting group, since they're asking us today to hold more consultations and that they be permanent and ongoing depending on how the bill evolves.

Mr. Balsillie, almost all the comments you've made on this bill thus far have been negative. Can you see anything anywhere in this bill that might be positive, or do you think we should simply toss it out and start over?

Based on what we have before us today, I think we've confused "privacy" with "artificial intelligence". These are two completely different things, but we're putting everything in the same basket.

We would've liked to hear what you had to say about artificial intelligence. I'm convinced you would have liked to talk to us about that at greater length as well. So allow me to give you the floor.

[English]

Mr. Jim Balsillie: Yes, I would like to put the sock on first with AI.

First of all, I said in my testimony that we should start over with AI. I agree.

Second, I think that the tribunal should be scrapped. There's no purpose for it other than to undermine the effective process. I do think that the privacy provisions can be fixed, but you have to fix them comprehensively. That's why I used the allegory of a bucket. If you leave one or two holes in a bucket, it's not a bucket, but you can patch all the holes. It is not a bargain to say, "I'll give you 10 holes to fix, but I'm going to leave 10 holes." You can patch all the holes in the privacy act, but you must do it. There's no reason that I can see that's legitimate for the tribunal. I think that artificial intelligence is so central and so comprehensive that it has to be done right or it will be forever toxic.

[Translation]

Mr. Bernard Généreux: I'd like to address the representatives of the Canadian Chamber of Commerce.

I'm a businessman. I have 40 employees in my various businesses, and we're awash in bureaucracy and red tape. Do you think that businesses with 100 employees or less, for example, a figure that appears in other bills, shouldn't be subject to the act or that they should be subject in a different way?

We know that small businesses are the economic backbone of this country. Should they be treated differently?

Ms. Catherine Fortin LeFavre: That's a good question. We didn't address it in our remarks.

Are you referring to the bill as a whole or to the part concerning the Artificial Intelligence and Data Act, or AIDA?

Mr. Bernard Généreux: I'm thinking particularly of certain provisions that might force businesses to deal with a lot of red tape to comply with the act.

● (1730)

Ms. Catherine Fortin LeFavre: We always take care to improve the process and help small businesses survive.

I'd like to put that question to our members, but I can tell you that, generally speaking, if we think a measure may help small businesses, then we support it.

Mr. Bernard Généreux: Ms. Vipond, have you been consulted?

[English]

Ms. Siobhán Vipond: This is, I guess, part of that process, but we think there can be a more meaningful way to do things at the table because, as we said, we're very concerned that the design is going to undo and go against human rights if AI is—

Mr. Bernard Généreux: My question is whether you've been consulted on this piece of legislation.

Ms. Siobhán Vipond: I guess we're here, but, yes, we think it could be more.

[Translation]

Mr. Bernard Généreux: The minister says he has met with 300 organizations and individuals. You said you had three million members in various sectors across Canada, didn't you?

Ms. Siobhán Vipond: Yes.

Mr. Bernard Généreux: But you were never consulted.

Ms. Siobhán Vipond: No.

The Chair: Thank you, Mr. Généreux.

Mr. Turnbull, the floor is yours.

[English]

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

Thanks to all the witnesses for being here today. It's a very useful discussion.

Ms. Krugel from the banking association, maybe I'll start with you. I think the banks generally have a clear understanding of what the CPPA will look like federally. From your perspective, will this bill help raise the floor for businesses across the country?

Ms. Lorraine Krugel: We believe the CPPA takes what's best from PIPEDA and strengthens it.

We also think that it's very important that the federal law be a guiding principle when the provinces start their privacy reform. Obviously, Quebec has done theirs already, but we know there are other provinces that are looking to do their own thing. It would be very helpful to have consistency and interoperability, so it would be in the best interests of organizations of all sizes, and also consumers, to have a consistent experience across provinces and federally.

Mr. Ryan Turnbull: Do you think that's possible with the way the bill is already worded?

Ms. Lorraine Krugel: It would be, with some targeted amendments, which we have put out in our proposal.

Mr. Ryan Turnbull: Thank you for that.

Ms. Clodman, I hear your point about consent fatigue. I thought that was a really good point. I personally have experienced that, although obviously informed consent is very important.

I think the notion of norms came up earlier. In your opening remarks, you mentioned that consumers want protections. They also want services to be delivered intuitively. They also want to share data, and they kind of expect to receive discounts or expect that at least that data will help provide them with discounts—and often that is kind of implied. People also value personalization. I think many of us can probably agree that this is part of the norms that exist out there today in terms of consumers' behaviour and their relationships with different types of businesses.

From my perspective, based on your comments, it sounds as though it is contrary to what Mr. Balsillie said about it being a balance. Could you speak to that balance and getting it right a little bit more?

Ms. Sara Clodman: Absolutely. Thank you for the question.

It is very important to remember that this bill has two purposes. We believe both of those purposes can be fulfilled in harmony. One is to protect consumers' personal information, which is extremely important. The other is to enable businesses to succeed and innovate.

What we need, at the end of the day, is to make sure that, in a situation where a customer would not expect their data to be used in a certain way, that consumer has the opportunity to express consent and agree to the use of their data. However, in cases where a consumer would expect their data to be used in a certain way for regular business activities, they should not be asked to consent. That is when consent fatigue happens.

Mr. Ryan Turnbull: I can see how that makes sense.

I can also see the flip side. There are some drawbacks to that, potentially. How do we know what consumers expect? We would need to have quite a lot of information about that.

Do you feel confident that this bill is getting it right, in terms of how it's defining "legitimate interest" in the various clauses? I think they imply some understanding of where those boundaries are.

• (1735)

Ms. Sara Clodman: The bill requires organizations—including not-for-profits looking to find funders and communicate with those funders—to make decisions about whether it is a regular activity. If they make the wrong decision, they are subject to significant fines under this bill, and to orders from the commissioner that can require them to stop collecting and using data. There is also reputational damage and the potential of a private right of action. Those are very significant incentives for companies to get it right.

Mr. Ryan Turnbull: Thank you for that.

Mr. Boms, I think we haven't shown you enough love today. It seems as if the people in the room have gotten the preference. I want to ask you a question.

You described, in your opening remarks, some significant benefits to the right of data mobility and portability included in CPPA. Can you elaborate further on some of those? Is there anything you didn't have a chance to say in your opening remarks that you could put on the record?

Mr. Steve Boms: Thank you for the question.

Indeed, data portability in the financial services context bestows upon a consumer or an SME the ability to choose the tool, product or service that is best suited for them. There is not nearly as much competition in the financial services sector in Canada as there exists in multiple other jurisdictions. Because Canada does not have this data portability right, consumers and SMEs in Canada may find themselves stuck with their current service provider, which doesn't help push down fees or improve services, products and tools. It can also be a significant barrier to SMEs and consumers trying to improve their financial life if they can't find the tool or product that is best suited for them.

The data portability right, in our view, brings Canada on par with many other countries that have gone further than Canada has, so far.

Mr. Ryan Turnbull: Thank you.

[Translation]

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

Mr. Falk, you now have the floor.

[English]

Go ahead.

Mr. Ted Falk (Provencher, CPC): Thank you to all the witnesses for coming here.

Mr. Balsillie, I'd like to start with you.

In your comments and responses to questions, you talked a lot about personal privacy, surveillance and protecting prosperity. When you were the co-CEO of BlackBerry, you demonstrated that. I don't think there's anybody in this room who has been the custodian of more personal private data than you have been, so you're speaking from a position of authority, experience and knowledge. You prioritized individual security and privacy for people. Ten years ago, when I became an MP, BlackBerry was the only option we had for telephones because of the security aspect of it.

During COVID, this government, together with their NDP coalition partners and through the Public Health Agency of Canada, colluded with Telus to trample on Canadians' individual privacy by tracking them. Is that the kind of thing you're concerned about with this legislation, that it doesn't protect Canadians from that kind of behaviour? They did it without a judicial authorization.

Mr. Jim Balsillie: If I may, I'm going to answer this a little indirectly. I dialogue a lot at the subnational level with premiers who are grappling with issues of data and identity systems and so on. People like to talk about efficiency. I explain to them that they must first invest in trust in governance. Somebody can't build a 20-storey skyscraper in your backyard without talking to you. You are all politicians who go through policy discourse, yet when it comes to these digital realms, there's a tendency to bypass the trust in governance phase, yet the power and impact are profound.

The most important things are the elements of dialogue, the elements of transparency, the elements of governance, so that people know that they can trust what you're doing and that there's going to be democratic recourse if you slip over the line. That's okay, but if you come top-down or if you do it absent transparency or with sneaky carve-outs, it collapses trust, and that shuts down a lot of things.

Independent of the harms these things do, you lose the social licence to move ahead in an era when we need social licence because we can't ignore the potential of these digital technologies to help us in a pandemic. However, there's a proper way to do these things, and there's an undermining way to do these things.

● (1740)

Mr. Ted Falk: Ms. Fortin LeFavre of the Canadian Chamber of Commerce, you said that you really hadn't consulted with members as to how they would feel about the additional reporting requirements that this bill would demand of small businesses. What do you expect the response to be?

I know that when the CFIB recently came to my office and gave me responses from the members they had in my riding, they reported back that one of the biggest concerns that small businesses have is the reporting requirements and the red tape. Did you get the same feedback through your members?

Ms. Ulrike Bahr-Gedalia: I'd gladly jump in here. Thank you for the question, Mr. Falk.

As the Canadian Chamber of Commerce, we don't have a large number of small businesses that we represent. Though it is very diverse across sectors and across jurisdictions and industries as well, the few that we have engaged with haven't really commented on it, if I may say so.

We do engage in consultations with all of our members. I'm leading most of the innovation and digital economy files and committees through that. I haven't heard back in particular, I must say, from the portion of the small to medium-sized businesses. However, you may wish to define them. I think there was mention earlier of 100 employees or fewer. It depends sometimes on the jurisdiction. Having resided in Nova Scotia for a long time, I think it was even less than that.

They have not been proactively participating in the dialogue, but I can envision that there are great burdens that they would attach to any reporting and so forth. However, I can't comment, and shouldn't, on their behalf, as they haven't voiced it as such.

[*Translation*]

The Chair: Thank you very much.

Mr. Villemure, the floor is yours.

Mr. René Villemure: Thank you, Mr. Chair.

Mr. Balsillie, you discussed the difficult interoperability with Europe in the context of Bill C-27. Could you be more specific on that subject?

[*English*]

Mr. Jim Balsillie: Absolutely.

First of all, I was commenting on adequacy. You have to maintain a threshold to interact with Europeans in the Canadian realm. When you look at the elements, very simply, of how you deal with children's data and how you deal with political party data, I don't believe that would survive a test.

Politicians can talk all they want, but if it goes to court and the judge says...just like they did in the Schrems II decision, you get shut down, and then you have to fix it in an emergency. Again, why not do it right the first time to protect Canadian business and Canadian citizens?

Just do it right.

[*Translation*]

Mr. René Villemure: In its present state, do you think Bill C-27 would be a good act when you consider generative artificial intelligence, better known as ChatGPT?

[*English*]

Mr. Jim Balsillie: No. I think what's happened since the original draft of this is that generative technologies have come to the fore. We used to think of data...and then you run an algorithm against it to get a result. Now you have data and an algorithm trains off it and says goodbye.

I will say—and this is beyond the scope of this committee—that you now have to think of what the infrastructure of a sovereign country is, because Europe has done what's called Gaia-X, a sovereign cloud. They're doing sovereign language models, because just to protect your data, but not control the rest of it.... In a sense, it'd be like us having our water treatment but not having our sovereign waste-water treatment. What is a sovereign country in an era of data and generative AI? We have to start thinking of what is national infrastructure and what is sovereign infrastructure. I chaired a panel on this subnationally, and I would extend it to the infrastructure, given what's developed in the past year, but our mandate was done a year ago. Yes, we have to get on with it.

Europe's been doing sovereign infrastructure with Gaia-X, with two billion euros for four years. They have their big summit next week in Spain. They have hundreds of companies. They have an interoperability framework. They have a permissions framework and an index of sharing. We should just draft right off it. We could do it federally and provincially. It's open-source. Infrastructure has to be talked about as part of this digital realm of data. It's there.

• (1745)

[Translation]

Mr. René Villemure: You're talking about adequacy. As we all know, adequacy is a form of social capital.

Unless we act or perhaps completely redo Bill C-27, do you think that social capital would be threatened?

[English]

Mr. Jim Balsillie: Yes. I chaired a panel on data authority for the Province of Ontario and I've been talking to them. In these elements of new privacy legislation and digital sharing protocols, it's a persistent structured form of consultation, including labour, including parents and including all kinds of communities, so that the licence has to be developed and maintained, because this moves laterally.

Yes, I think social licence needs to be a central part of the ongoing operating realm of data, in both public and private sectors.

[Translation]

Mr. René Villemure: Thank you very much.

Mr. Elder, you are a privacy law expert. In your opinion, when an average user clicks on "Accept", does he actually understand the end use of his consent?

[English]

Mr. David Elder (Head, Privacy and Data Protection Group, Stikeman Elliott LLP, Canadian Marketing Association): I'm sorry. I missed part of that. I wasn't getting the volume.

I apologize.

[Translation]

Mr. René Villemure: I'll repeat.

Do you think an average user understands the end use of his consent when he clicks on "Accept"?

[English]

Mr. David Elder: I think it depends very much on the scenario you're talking about. Sometimes there are some pretty simple data uses. We have to remember that this bill, for example, covers a wide range of industries and businesses, so certainly in more simple transactions, I would think that, in many cases, the answer would be yes. If you're talking about a more complicated transaction and use of algorithms, I'm not sure that the average user would always necessarily understand—

[Translation]

Mr. René Villemure: For example, when a citizen or user clicks "Accept" on the website of Le Figaro, the newspaper, is he able to understand how his data will ultimately be used?

[English]

Mr. David Elder: I suppose it depends on whether they've read the document to which they're consenting and understand the privacy policy.

[Translation]

Mr. René Villemure: All right.

Thank you, Mr. Chair.

The Chair: Thank you, Mr. Villemure.

[English]

I'll now yield the floor to MP Van Bynen.

I'm sorry. I skipped you in the last round, but the floor is yours, MP Van Bynen.

I went from Mr. Falk to Mr. Villemure, but it should have been MP Van Bynen.

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

My question will be for Ms. Krugel.

Particularly with respect to the Canadian Bankers Association, what barriers would an organization have to overcome to meet the new obligations under the consumer privacy protection act?

Ms. Lorraine Krugel: Are you asking what the net new obligations are compared with those of today?

• (1750)

Mr. Tony Van Bynen: Yes. How substantive are they in terms of implementation, and what would it take?

Ms. Lorraine Krugel: There are a number that are actually quite substantive. PIPEDA is very principles-based. Organizations have been able to scale what they do according to the circumstance.

The CPPA takes inspiration from the GDPR and the law in Quebec, and some of the key concepts are very prescriptive. Some of those can be very.... It can take a lot to implement. For example, relating to the automated decision system, this is a provision that goes beyond what the GDPR and Quebec do. Both Quebec and GDPR only focus on scenarios that are exclusively automated, and the organization would need to tell the individual when a decision is solely automated.

Under the CPPA, organizations will have to consider all of the automated systems, which could be AI systems or even an Excel spreadsheet that is automated, and have an understanding of whether they assist in the decision-making or in making a prediction or a recommendation. There's a lot.... The organization would need to take a look at almost everything they do and be prepared to provide explanations to individuals. With respect to training and understanding all of these processes, it can be quite cumbersome.

That's one element.

Mr. Tony Van Bynen: There's a discussion about a two-year cycle for implementation. Is that correct?

Ms. Lorraine Krugel: Yes. Some of these requirements—any changes to consent and anything that requires changes to a system—can have a very long runway, particularly in larger, complex organizations. Even printing out new consent forms and ordering paper can be very time-consuming, as well as getting access to legal experts to make sure you understand the requirements, particularly if there are differences between federal and provincial requirements—and technology resources as well. There are scarce resources that need to be shared among all organizations to be able to understand requirements to comply.

Mr. Tony Van Bynen: Proposed sections 76 to 81 of the consumer privacy protection act would provide for a procedure allowing organizations that are subject to the act to create codes of practice and certification programs that would go to the Privacy Commissioner for approval.

Would your organization submit a code of practice to the Office of the Privacy Commissioner that would apply to all of your members? Would that be your intention?

Ms. Lorraine Krugel: It would depend. Certainly a code of practice could be beneficial if there were a certain area where there was a potential for differing interpretations of what is required. It could set out rules that organizations would follow.

Basically, there would be additional trust provided by the Privacy Commissioner, to say this is the type of approach that would be supported under the CPPA. It could provide trust to consumers that it has been reviewed, and also trust and certainty to organizations. Whether or not the Canadian Bankers Association would choose a specific code of practice, we haven't gone down that far just yet.

Mr. Tony Van Bynen: Okay.

I understand that your organization does have codes of practice in terms of certification for investment advisers, etc.

Ms. Lorraine Krugel: No, it's not under the Canadian Bankers Association. The banking industry does have some codes of practice, and I think it's also with respect to credit practices.

Mr. Tony Van Bynen: I'd like to go with the same question to Ms. Clodman.

In terms of your organization, would you be instituting codes of practice that would be subject to the approval of the Privacy Commissioner?

Ms. Sara Clodman: We haven't made a final decision yet about that.

We were talking about a code of practice around marketing. We already have the “Canadian Marketing Code of Ethics & Standards”, and also possibly one related to the use of children's data. Again, we have that in place and have had it for many years.

Mr. Tony Van Bynen: That is the reason I wanted to approach you on that. You have established your own code, so I was trying to determine your intent with respect to setting the same standards.

Setting up those certificate programs goes back to the values-based principles that you want organizations to accept. I was trying to get a better understanding as to whether or not the two organizations that you represent would be pursuing the values-based principles in applying...your consideration as to how you would go forward with this.

Go ahead.

Ms. Lorraine Krugel: With respect to a code of practice, we understand, too, that there might be certain very narrow scenarios that could really benefit from a code of practice. For example, information sharing could be something that's very specific.

Generally speaking, for the banking sector, each of our banks has very robust privacy management programs already in place under PIPEDA, so we wouldn't necessarily look to create a code of practice for all compliance for the CPPA, although we could see some very good benefit for small and medium-sized businesses, for example.

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

The Chair: You're over by a minute and 20 seconds, Mr. Van Bynen. Thank you very much.

For our final round of questions, I'll yield the floor to Ms. McPherson.

Ms. Heather McPherson: Thank you very much, Mr. Chair.

Again, thank you to all the witnesses for their testimony today.

Mr. Balsillie, in your brief, you recommended establishing a complaint-funding mechanism to help finance legal proceedings brought by individual or group complainants and/or public interest organizations seeking remedies against organizations for alleged contravention of the CPPA. Can you explain why this is important and why it's essential to this regulatory process?

• (1755)

Mr. Jim Balsillie: There's a structural asymmetry in the nature of this evidence, where you click a consent where somebody writes a sophisticated consent and then somebody does click, or the individual doesn't have the ability to exploit their data, but a large company can. There's also a marked failure in the ability to follow through on a complaint. What you're really trying to do here is create rebalancing mechanisms so that the public good is served.

Ms. Heather McPherson: To make sure I have this right, could you explain why a private right to action is important, as has been the case in other jurisdictions, such as the United States?

Mr. Jim Balsillie: An individual who thinks they've been harmed has the ability to file a complaint and use the judicial system to say that they've been harmed and not appeal to a busy regulator that is grappling with budget constraints, multiple priorities and possibly different points of view based on their circumstance.

Ms. Heather McPherson: Thank you.

Perhaps our guests from the CLC would also like to comment on that.

Ms. Siobhán Vipond: I'm sorry. Could you repeat the question for me?

Ms. Heather McPherson: It's about the idea of using a complaint-funding mechanism to help finance legal proceedings. The question is whether or not you would be in agreement with that.

Ms. Siobhán Vipond: Absolutely, there needs to be an ability for folks to work through it and make a complaint, but we have to make sure that, when that happens, the right people are listening to it so there's an ability to respond in a reasonable way.

Ms. Heather McPherson: Thank you.

Ms. Vipond, has the CLC considered specific changes to this bill that would help to include labour laws or provisions to ensure that the concerns you've raised are addressed? Could you elaborate a little bit on those? Are there other countries or jurisdictions that have done so that you would be considering when you include these?

Ms. Siobhán Vipond: I will say that one of our recommendations is that AIDA should be reconceived, and that's from a human, labour and privacy rights-based perspective so that we can place transparency, accountability and consultation at the core of the approach to AI, which is not what we see in front of us, so that is a big ask.

We are looking to that executive order in the United States as having better language than we're seeing. We also see examples in other jurisdictions where it's being approached from a social dialogue sense. We do have many asks about this, but I think, fundamentally, that is a big one.

I need to reiterate that we have to expand who's covered and that the government and Crown corporations cannot be excluded. That comes from a workers' rights perspective.

Ms. Heather McPherson: Thank you.

I have a last question for you. What recourse mechanisms still missing in the bill with regard to algorithms or data collection, use and permissions that could impact the relations between employers and employees would you like to see included in this bill?

Ms. Siobhán Vipond: We hear lots of workers telling us about how AI is being used in terms of surveillance in the workplace, and as a human rights issue, when the process excludes a person. There's actually no human intervention in that process, which is a huge concern for us. That is one of the big things we're looking at when we're talking about what needs to be addressed here.

The mechanisms that are currently laid out in AIDA don't give us enough opportunity to talk about that and regulate it, because unregulated goes unchecked, and then we're going to fall into a position where human rights, including workers' rights, are not going to be respected.

Ms. Heather McPherson: Thank you very much.

That's all for me, Chair.

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

We're almost done, but Mr. Perkins has one last question. I trust it will be short, Mr. Perkins.

Mr. Rick Perkins: That's a challenge for me.

I'd love to ask the Canadian Bankers Association something, but maybe I'll leave that until after.

Mr. Balsillie, who owns somebody's data? Is it the individual or the company?

Mr. Jim Balsillie: You can't really own data; it's about control of the data. The question of who's allowed to collect it in the first place...that's lawlessness. We're living in a lawless world right now, so people are just doing it without any real laws that say what you're allowed to do in the first place.

It's colonizing personal space. That's what's happening in lawlessness right now.

• (1800)

Mr. Rick Perkins: To the Canadian Bankers Association, you mentioned proposed section 35 earlier, which I did as well. The current Privacy Act limits that power to use it without knowledge for research and statistics to academic-type things. This complete replacement leaves it wide open because it just says “an organization”; it doesn't limit it to scholastic or academic organizations.

Could you comment on that?

Ms. Lorraine Krugel: Actually, we did not provide any recommendations relating to that one.

What is the concern about that one?

Mr. Rick Perkins: Proposed section 35 says, “An organization may disclose an individual's personal information without their knowledge or consent” if it's used “for statistical purposes or for study or research purposes”, which is pretty wide open. Previously, PIPEDA limited it to scholarly work. That leaves it open to anybody—any organization—to do it without consent, in my view.

Ms. Lorraine Krugel: I'm not sure that that would be a provision that our members would be looking to leverage for the internal research and analysis that they do.

Mr. Rick Perkins: I can tell you that, as a former bank marketer, I would exploit that very well.

The Chair: We'll leave it at that, Mr. Perkins.

[Translation]

Mr. Bernard Généreux: I have a point of order, Mr. Chair.

With your permission, I'd like to thank the witnesses who are here today. We have heard from high-quality witnesses since we began our study. I'm raising a point of order because I would like us to have more time with them. To do so, if possible, we would have to hear from fewer witnesses at our next few meetings.

The Chair: That's understood, Mr. Généreux.

We have heard from six panels of witnesses, which is remarkable. We normally have five. We've invited more in order to be sure of having diversified witness panels, as was the case today.

I want to thank the witnesses for their time; we are grateful to them for that. Thank you for enlightening us.

With that, I want to thank the interpreters, our support staff, analysts and the clerk.

The meeting is adjourned.

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

SPEAKER'S PERMISSION

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

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

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

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

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

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

PERMISSION DU PRÉSIDENT

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

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

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

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

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