HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

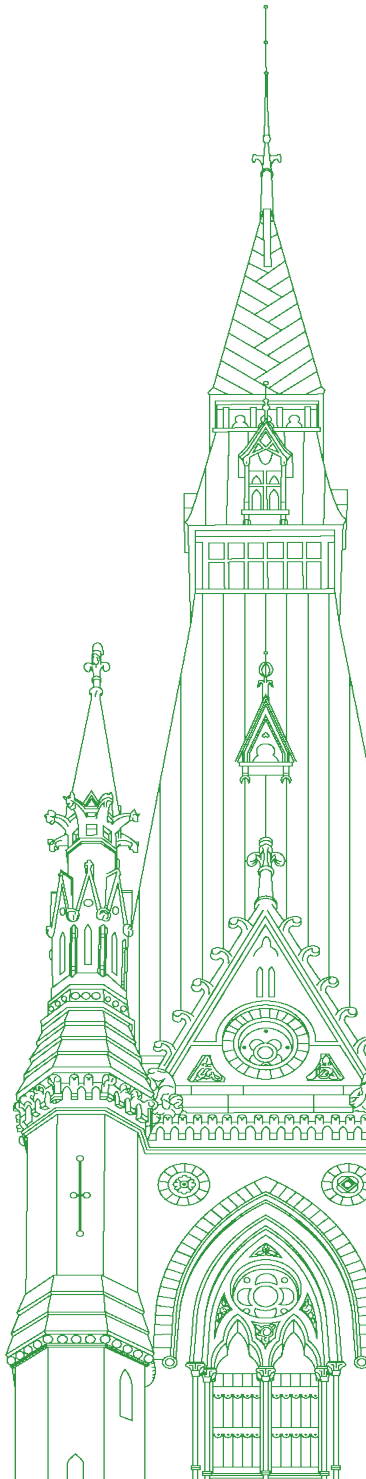
44th PARLIAMENT, 1st SESSION

Standing Committee on Industry and Technology

EVIDENCE

NUMBER 091

Tuesday, October 24, 2023



Chair: Mr. Joël Lightbound

Standing Committee on Industry and Technology

Tuesday, October 24, 2023

● (1530)

[*Translation*]

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

Good afternoon. Welcome to meeting number 91 of the House of Commons Standing Committee on Industry and Technology.

Today's meeting is taking place in a hybrid format, as per the rules. Pursuant to the order of reference of Monday, April 24, 2023, the committee is resuming its study 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 witnesses today. We have, appearing as individuals, David Fraser, partner at McInnes Cooper; Éloïse Gratton, partner and national leader, privacy and data protection, at BLG, who is joining us by video conference; and Daniel Therrien, lawyer and former Privacy Commissioner of Canada. Ms. Gratton was my professor at Université de Montréal for a short time, so it's nice to see her again. Finally, from the Canadian Anonymization Network, we have Adam Kardash, partner, and Khaled El Emam, professor, both joining us by video conference.

Thank you all for being here today.

We are fortunate to have this panel for our study of Bill C-27, so without further ado, I will turn the floor over to Mr. Fraser for five minutes.

[*English*]

Mr. David Fraser (Partner, McInnes Cooper, As an Individual): Thank you very much, and thank you for your kind invitation to appear before this committee to assist in its important study of Bill C-27.

I'm a partner in private practice at a law firm where I've been practising privacy law for 22 years. Most of my practice involves advising international businesses on complying with Canadian privacy laws. More often than not, they're trying to make their existing privacy programs, which they've developed in places like Europe and California, work in Canada. I also advise Canadian businesses, large and small, on compliance with these laws. I regularly advise organizations in connection with investigations and encounters with the Office of the Privacy Commissioner of Canada and his provincial counterparts.

I'm here in my own personal capacity, but obviously my work and opinions are informed by my experience working with my clients.

Now, I may come across as somewhat contrarian in saying this, but I actually think that PIPEDA works pretty well as it is. It was designed to be technologically neutral, based on existing principles that are largely embedded in Bill C-27. One thing I've often said is that Bill C-27 takes PIPEDA and turns it up to 11.

I don't think the legislation's necessarily broken. I think the commissioner, over the past 22 years, has not necessarily exhausted all of his enforcement powers and authorities over that time.

I'd like to start by saying that I don't really like the name of the new statute. Canadians aren't simply consumers. This legislation applies to consumers. It also applies to certain employees in the federally regulated sector. It's a bit negative and dismissive. If we're wedded to the acronym CPPA, we could call it the “Canadian Privacy Protection Act”, but I don't think that actually affects its substance.

Now, I like PIPEDA, but over the last little while, it's been pretty clear that there's an emerging consensus in looking toward order-making powers and penalties and thinking they're desirable. In the course of this, I would ask the committee to consider that that requires a commensurate and appropriate increase and shift to greater procedural fairness than is currently in the bill.

Based on my experience, I'm of the view that the Privacy Commissioner potentially has a conflict in being a privacy advocate, a privacy educator, the privacy police, the privacy judge and the privacy executioner. Any determination of whether a violation of the CPPA has taken place and what penalties should be imposed should be carried out by an independent arm's-length tribunal, such as the Federal Court or the new tribunal. The commissioner can recommend a penalty and can take on the role of prosecutor, but ultimately the determination of whether or not a violation has taken place and whether or not a penalty should be imposed should be vested in an arm's-length body.

I think the recent Facebook case in the Federal Court is a bit of a cautionary tale. I'd be happy to talk more about that.

Children's privacy is obviously a very important theme in this particular piece of legislation. I agree with and appreciate the views of the government and the commissioner with respect to protecting the privacy of children.

One thing I'm a bit concerned about is that the current bill would be difficult to operationalize for businesses that operate across Canada. Whether or not somebody is a minor currently depends upon provincial law. That varies from province to province, and implementing consistent programs across the country would be difficult. I would advocate putting in the legislation that a minor is 18 years or below.

I would also suggest that there be a presumption that children under the age of 13 are not able to make their own privacy decisions and that their parents should be their substitute decision-makers by default.

For organizations that offer a general service to the public—like a car dealership, for example—there should be a presumption that all of their customers are adults, unless they know otherwise. If you have a website that's focused toward children, you know there are children in the audience and you have to calibrate your practices appropriately. Anything different might lead to mandatory age verification, which can be very difficult and raises its own issues.

Having been involved in investigations and in litigation involving privacy claims, I would suggest that the “private right of action” be amended to be limited to the Federal Court of Canada, if you're wedded to a private right of action to begin with. The problem with the existing legislation is that anybody can go to the Federal Court of Canada or a provincial court. We know that there are going to be hundreds of people affected over the next decade or so, with respect to particular incidents. You're going to end up with duplicative proceedings simultaneously across the country. We already know that judicial resources are significantly taxed.

I think legitimate purposes—which are largely based on the European model—need to be more closely aligned. I'm happy to provide more details on what is happening in Europe.

With respect to the artificial intelligence and data act, it should be its own bill and subject to its own study. I would note that excluding the government from it is dangerous. The government has guns. The government decides about benefits, immigration and things like that. I think it's subject to a constitutional challenge. It's not necessarily harmonized with what's going on with our international trading partners, and there should be reciprocal recognition.

● (1535)

If a company is complying with European data regulation and we have deemed it to be substantially similar, that should work. Otherwise, we're going to have difficulty with Canadian businesses operating internationally and international businesses coming here.

Finally, I think research and development should be removed from the bill, because it presents no real risk of harm to an individual until it's presented into the public.

I have a longer list. I could go on for much more than five minutes, but I think that's my time. I look forward to the discussion.

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

I'll now turn to Madam Gratton for five minutes.

[*Translation*]

Ms. Éloïse Gratton (Partner and National Leader, Privacy and Data Protection, BLG, As an Individual): Thank you for inviting me.

I'm pleased to be here today to share my thoughts on Bill C-27.

I am a partner at Borden Ladner Gervais and the leader of the firm's national privacy and data protection practice. Having worked in the field for more than two decades, I provide advice to large national companies in a number of industries across the private sector. Many of these companies have international operations as well, so I have followed the developments in the European Union's General Data Protection Regulation, or GDPR, in recent years. The GDPR is, of course, the EU's equivalent to our privacy legislation.

I believe this privacy reform process should draw on the lessons learned by Quebec and the European Union in reforming their privacy legislation.

I am here today as an individual. I'm going to switch to English now, but I would be happy to answer members' questions in English or French.

[*English*]

Today I stand before you to discuss a matter of paramount importance, the reform of the federal privacy law.

We find ourselves at a critical juncture. We have the unique opportunity to strike a balance that ensures the protection of our privacy rights while fostering an environment of innovation. In a rapidly evolving digital age, where information flows faster than ever before, our privacy is at an increased risk. This makes it imperative that we reform our privacy laws to reflect the realities of today.

However, data protection laws should not stifle the innovative spirit that has propelled us into the 21st century. Canada needs to remain competitive. Innovation drives economic growth, creates jobs and improves our quality of life. It is the engine of progress. Striking the right balance between privacy and innovation is a complex task, but I don't think it's an impossible one.

I'll focus my presentation on the consumer privacy protection act and areas of improvement for four specific issues that potentially impact innovation.

First, I absolutely welcome the introduction of a consent exception regarding specified business activities and for certain activities in which the organization has “legitimate interest” under subclause 18(3). This being said, the legitimate interest exception is actually narrower than the same exception under the EU's GDPR, the General Data Protection Regulation.

David raised this issue, so I'm going to talk a bit more about it.

Bill C-27 provides no exception, nor any significant flexibility, as to the application of the consent rule to the collection of personal information collected from publicly available sources on the Internet. It prevents all organizations from leveraging data available on the web, including legitimate ones working on new products and services that may benefit society and that need a large volume of information.

In short, I submit to you that this legitimate interest exception should be more closely aligned with the GDPR legitimate interest legal basis to accommodate innovative types of business models while protecting the privacy interests of Canadians.

Clause 39 creates a new consent exception for disclosures of de-identified personal information to specific public sector entities, including government, health care and post-secondary educational institutions. Limiting this consent exception only to disclosures to public sector entities instead of public and private sector entities severely restricts its utility. Clause 39 should authorize and facilitate responsible data sharing between a broader range of actors to have access to talent and resources that they can leverage to pursue socially beneficial purposes.

The third point is that the CPPA introduces new definitions for the terms “anonymize” and “de-identify” and provides greater flexibility regarding the processing of these categories of information. However, the proposed standard for anonymization under subclause 2(1) is more stringent than other recently updated privacy legislation, including the GDPR and the recently amended Quebec private sector act.

My point is that the CPPA should include a reasonableness standard instead of holding organizations accountable to an absolute standard that may be impossible to meet in practice. As you certainly know, access to to anonymized datasets, with legal certainty, is crucial to research and development performed by Canadian organizations. I have a feeling that Adam Kardash and Khaled El Emam will be talking about this a bit more.

My last point is that clause 21 introduces a new consent exception for the use of de-identified information for internal research, analysis and development purposes.

● (1540)

Restricting such use to internal uses may limit collaboration and the fostering of research partnerships, preventing stakeholders from sharing datasets to create data pools that are broad enough for the production of useful and actionable insights. This section should authorize the use and sharing of de-identified information among different organizations.

I've submitted a short brief in French and English in which I provide additional detail on these four proposed changes. I think innovation and privacy can coexist, and the responsible use of personal information can be the cornerstone of building new and exciting technologies while respecting our fundamental rights.

Thank you, and I welcome questions.

[*Translation*]

The Chair: Thank you, Ms. Gratton.

We will now hear from Mr. Therrien for five minutes.

Mr. Daniel Therrien (Lawyer and Former Privacy Commissioner of Canada, As an Individual): Thank you, Mr. Chair.

Thank you, committee members, for inviting me to participate in your study.

I am here as an individual, but my experience as the federal privacy commissioner from 2014 to 2022 will certainly be reflected in my remarks.

To begin, let me say I agree with my successor, Philippe Dufresne, that the bill before you is a step in the right direction, but that it is necessary to go further in order to properly protect Canadians. I also agree with the Office of the Privacy Commissioner's 15 recommendations for amending Bill C-27, with some nuances on audits, remedies and appeals. The government has taken up, at least in part, a good number of the recommendations I had made regarding Bill C-11, the predecessor to Bill C-27. Among those that were not accepted is the application of privacy law to political parties.

I am very pleased that a consensus appears to have emerged among political parties to recognize in the law that privacy is a fundamental right. I applaud parliamentarians for that decision. The question now becomes how to best translate into law the principle with which you now all agree.

● (1545)

[*English*]

Minister Champagne suggests amending the preamble and the purpose clause of the CPPA. These are steps in the right direction, but they are not sufficient. You should also amend two operative clauses: proposed section 12 of the act on “appropriate purposes”, and proposed section 94, which provides for administrative monetary penalties for certain violations of the law. Without these amendments, the law would still give greater weight to commercial interests than to privacy, which is a fundamental right. This does not appear to be your intent.

Based on my reading of parliamentary debates, it also seems to me there's consensus around the idea that privacy and economic growth through innovation are not in a zero-sum game. The question is generally not on deciding which should prevail—privacy protection or innovation—as both can and should be pursued at the same time. It is only in rare cases that it will not be possible. In those cases, privacy as a fundamental right should take precedence.

Proposed section 12 of the CPPA does not, in my view, faithfully translate this consensus. Rather, it upholds the traditional approach, which is that privacy and economic goals are conflicting interests that must be balanced without considering that privacy is a fundamental right. This may have made sense under the current act's purpose clause, but it will no longer make sense if the CPPA's purpose clause recognizes privacy as a fundamental right, as is currently proposed.

Proposed section 12 is central to the exercise that commercial organizations, the Privacy Commissioner and ultimately the courts will have to go through in order to determine the factual context of each case and the weight given to privacy and commercial interests.

[*Translation*]

Section 12 as drafted gives more weight to economic interests. It does that in several ways.

The first is through the terminology it uses. It refers to “business needs” and does not refer to privacy as a right, fundamental or otherwise.

When the proposed section does refer to privacy, in paragraphs (2)(d) and (e), it is as an element to consider in achieving business goals, mitigating losses where possible, that is where achieving business goals can be achieved at comparable cost and with comparable benefits.

Nowhere is it mentioned that privacy protection is an objective at least equally as important as economic goals. On the contrary, the focus is on economic goals, and privacy loss as something to be mitigated, where possible, in the pursuit of those goals.

I have provided you with my proposals for amending section 12, and they would be consistent with the amendments proposed at section 5.

With respect to sanctions, all violations of section 12, including the appropriate purposes clause at subsection (1), should potentially lead to administrative monetary penalties. Without sanctions, recognizing privacy as a fundamental right would be a pious wish, without real consequences.

I would go further and recommend that all violations of the CPPA should be subject to these penalties. This would align Canada with most other jurisdictions.

[*English*]

I have a few words on the Artificial Intelligence and Data Act. That part of Bill C-27 is brief, even skeletal, and leaves a lot of room for regulations. While I understand why some are concerned with this, I think this approach is defensible, given the fact that AI technology is relatively nascent and is certainly evolving very quickly; however, the lack of precision in AIDA, in my opinion, requires that certain fundamental principles and values be recognized in the act itself. First and foremost, the act should recognize the importance of protecting fundamental rights, including the right to privacy, in the development and implementation of AI systems.

Finally, some of you expressed concerns in an earlier meeting with the difficulty of detecting violations of the law and the potential value of proactive audits to facilitate detection. As commissioner, I had recommended proactive audits, and I still believe they are a necessary part of an effective enforcement regime. This is particularly true in the case of AI.

Thank you. I would be pleased to take your questions later.

● (1550)

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

Finally, from the Canadian Anonymization Network, we have Mr. Kardash.

Mr. Adam Kardash (Partner, Canadian Anonymization Network): Thank you. Good afternoon, everyone.

My name is Adam Kardash. I'm chair of Osler, Hoskin and Harcourt's national privacy law and data management practice, and I've been practising exclusively in the privacy area for more than 20 years.

I'm pleased to be before INDU on behalf of CANON, the Canadian Anonymization Network, which is a not-for-profit organization whose members comprise large data custodians from across the public, private and health sectors.

I'm joined this afternoon by Khaled El Emam, a Canada research chair in medical AI at the University of Ottawa and the leading global expert on anonymization and de-identification technologies and methods.

As you are aware, Bill C-27 introduces definitions of anonymized data and de-identified data within the text of the proposed consumer privacy protection act. The concept of anonymized data is a core feature of the CPPA, as it clarifies the scope of application of the CPPA's privacy legislative scheme.

There are several very important provisions throughout the CPPA related to the terms de-identification and anonymization. It is therefore essential that the CPPA provisions relating to these terms—anonymized and de-identified data—be carefully considered and appropriately articulated within the CPPA's legislative scheme.

In August of 2022, CANON struck a working group to conduct a thorough legal consideration of Bill C-27, and we received comments from stakeholders across all sectors as part of a consultation process, including a workshop attended by over 100 participants.

CANON is proposing surgical revisions that provide critical clarifications to several provisions within the CPPA, including to the provision referenced by my colleague Éloïse Gratton for proposed section 39. We're proposing additional privacy protections to disclosures without consent for socially beneficial purposes. The details of our submissions are contained within the written submission we submitted to INDU.

Our most important recommendation relates to the CPPA's current definition of “anonymize”. The current definition provides that personal information would be anonymized only if it is “irreversibly and permanently” modified in accordance with “generally accepted best practices, to ensure that no individual can be identified from the information, whether directly or indirectly....”

We are proposing an amendment as a surgical addition to this definition, as the current text of the definition of “anonymize” sets an extremely high and practically unworkable threshold for the circumstances in which information would no longer be deemed to be identifiable. Specifically, anonymized data within the CPPA does not incorporate the concept of reasonably foreseeable risk in the circumstances and therefore is not consistent with the standard for anonymization within legislative schemes across the country, including Quebec's Law 25, Ontario's Personal Health Information Protection Act, and multiple other statutes cited in our submission. We have everyone. There are at least 12 that we've cited in the statutes for your consideration when you're reviewing our brief.

To be clear, and this is critically important, there is a very high legal standard for anonymization right now in Law 25, under PHIPA and under all these other statutory frameworks. It's very high, but unlike the CPPA, the anonymization standard in these other legislative schemes is practically workable. The reason is that it expressly contemplates contextual risk.

As a result of these concerns, CANON has proposed an amendment to the CPPA's definition of “anonymize” that simply incorporates the concept of reasonably foreseeable risk in the circumstances into the definition. Our proposed surgical amendment would align the CPPA's concept of anonymized data and, critically, ensure the interoperability of the CPPA with the standard for anonymization within other legislative schemes across Canadian jurisdictions. Our proposal is fully consistent with well-established Canadian jurisprudence on the scope of the concept of personal information, the citations for which we provide in our submission.

I'm going to turn my comments over now to Khaled El Emam to conclude our introductory remarks.

Dr. Khaled El Emam (Professor, Canadian Anonymization Network): Thank you, Adam.

I want to use my time today to highlight the practical importance of CANON's proposals to the definition of “anonymize”.

My comments today are based on my experience with anonymization over the last two decades, both in the context of research and applications and of practice. A core focus of my work has been on the anonymization of health data such that it can be used and disclosed for research purposes, which includes developing new treatments and devices to help patients.

In my view, the CPPA's current definition of “anonymize” most often will not work well in practice when interpreted literally. It risks setting an unachievable standard that in practice is not necessary for good privacy protection. The text needs to reflect the reality that the outcome of anonymization is not absolute. It is well established among anonymization and data de-identification experts that data anonymization is a process of risk management. This is a foundational element of the recently published ISO international standard for data de-identification. Good contemporary practices, when implemented properly, can ensure that the re-identification risk is very small. Very small re-identification risk can be precisely defined and has been precisely defined by organizations such as Health Canada.

Effective re-identification risk management involves using techniques and technology to modify data as well as the implementation of appropriate administrative and technical controls. The combination of modified data that has been wrapped with appropriate administrative and technical controls ensures that the re-identification risk can be made very small.

This concept of risk management will not ensure that the re-identification risk is zero or that anonymized data is absolutely irreversible. That is not a practical standard that can be met. This is why it's important to amend the current definition of the term “anonymize”, which currently implies zero risk.

Our proposal supports the important and necessary requirement currently within the CPPA's definition that generally accepted best practices are followed during the process of anonymization, but the CANON proposal adds the concept of reasonably foreseeable risk and the circumstances so that the definition is actually workable in practice.

Based on my years of developing and implementing anonymization methods and technology, on behalf of CANON I think the implementation of CANON's proposals will enable a more responsible use and disclosure of data compared to the current definition.

We thank you in advance for your consideration. We would be pleased to answer any questions you may have.

● (1555)

The Chair: Thank you very much, Professor.

We'll start the discussion.

Colleagues, given that we have an hour and a half and a lot of witnesses, I will be stricter on time. Please look at me towards the end of your time.

Go ahead, Mr. Perkins.

Mr. Brad Vis (Mission—Matsqui—Fraser Canyon, CPC): Just for me, I get 10 minutes right?

The Chair: No, you don't, not today.

Mr. Perkins, without further ado, go ahead for six minutes.

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

My first series of questions are to Mr. Therrien.

You were the Privacy Commissioner during the development of the replacement for the Privacy Act in the last Parliament, Bill C-11, and presumably in the run-up to the development of this one. The current Privacy Commissioner was here last week and said essentially that he personally wasn't the commissioner who was consulted on it.

This is a critical bill because it's a complete replacement of the Privacy Act. It's not an amendment.

I'll start by asking you if, in the development of Bill C-11, the Minister of Industry of the day—I believe it was Mr. Bains—consulted with you before the bill was tabled in Parliament.

Mr. Daniel Therrien: We had a couple of discussions with Mr. Bains and Mr. Champagne. We never saw the actual text of the bill, but there were discussions.

Mr. Rick Perkins: However, Bill C-11 was tabled—

Mr. Daniel Therrien: Yes.

Mr. Rick Perkins: —and Bill C-27 was tabled.

Did either of those bills reflect the advice you gave them?

Obviously not, since you asked for a number of errors to be...but did they reflect the desire to have fundamental right included in the bill?

Mr. Daniel Therrien: I characterize Bill C-11 as a step backwards. I think Bill C-27 is a step forward. Some recommendations that I had made as commissioner were accepted—not all, and not some that I think are essential that I spoke to.

Mr. Rick Perkins: I assume you made a recommendation of fundamental right both times.

Mr. Daniel Therrien: Yes.

Mr. Rick Perkins: They were ignored both times.

Mr. Daniel Therrien: At that time, yes.

Mr. Rick Perkins: Now, 18 months after the minister introduced this bill, this flawed and broken bill, he's finally admitted after all of this process that it's a broken bill and he has to amend it eight times at fairly fundamental things.

I'll ask you on this issue of fundamental right what you believe about simply putting it in proposed section 5 on a parallel. Proposed section 5 is the most important section of the bill, because it supposedly says in the bill, when the amendment gets tabled, that protection of privacy is a fundamental right and that an organization basically has the right to use that data.

It appears to me that in proposed section 5, which is the thing that sets out the whole purpose of everything else in the bill, personal privacy is treated as being of equal importance to its use by a commercial entity.

Is that true?

● (1600)

Mr. Daniel Therrien: The first point I make is that it is important that proposed section 5 speak to and qualify the right to privacy as fundamental. It has meaning. However, you have to look at the whole of the purpose clause, the preamble first—

Mr. Rick Perkins: The preamble isn't in statute, though, once the bill has passed.

Mr. Daniel Therrien: Proposed section 12, which is actually the balancing exercise that actually occurs on a case-by-case basis, and proposed section 94, the penalty provisions, as a whole need to reflect the idea that privacy is a fundamental right. At this point, with the amendments tabled by the minister, we're doing well with proposed sections 2 and 5, but not with proposed sections 12 and 94.

Mr. Rick Perkins: I would say that proposed sections 12, 15 and 18 are critical on the privacy part. I agree that AIDA is a blank slate, and we'll come to that another time—hopefully today.

Proposed section 12 sets out the purpose. Proposed section 15 talks about express consent and then, in proposed subsection 15(5), says that it's okay to use “implied consent”. Then proposed section 18 says that a business has “legitimate interest” to use an individual's data basically however it wants, even if it harms the individual.

To me, it places the emphasis. When you take proposed section 5 and then add proposed sections 12, 15 and 18 to it, it looks like big business and its right to use your data is being protected in this, even if it harms you.

Do you not need to amend all of those proposed sections, not just proposed sections 5 and 12?

Mr. Daniel Therrien: I think that proposed section 15 on consent does need to be amended, and I speak to this in the document that I left with you.

On the concept of “legitimate interest”, I would give the following advice. This is a concept that exists in European law, which is considered to be the gold standard internationally. I think it is possible to have a “legitimate interest” type of exception to consent, provided that the sum total of proposed sections 2, 5, 12 and 94 actually do protect privacy as a fundamental right. There's no inconsistency between “legitimate interest” and considering privacy as a fundamental right.

Mr. Rick Perkins: However, without that—because the minister has not proposed that—

Mr. Daniel Therrien: Yes, we have a problem.

Mr. Rick Perkins: —we have a problem, absolutely.

I'd just like to ask Mr. Fraser a question in the little bit of time that I have left.

I think that AIDA is a problem because AIDA actually doesn't set out a public policy framework, which is what legislation is supposed to do. It just says, more or less, “Trust us; we'll do it all in regulation.” However, you mentioned that it would be perhaps open to a charter challenge. I wonder if you could expand on why.

Mr. David Fraser: The conclusion I draw on that is that it's simply saying within the legislation, or saying within the bill, that it applies to artificial intelligence in connection with interprovincial activities. The federal Parliament has very little jurisdiction, for example, over a computer science researcher sitting at the University of Toronto. That's exclusively within provincial jurisdiction.

There are going to be scenarios in which federal jurisdiction may be triggered, but in the vast majority of situations, such as when a small company in Nova Scotia or a small company in British Columbia decides to implement an artificial intelligence system, it's not within the competence of the federal Parliament when they do it on that small scale. Therefore, there are going to be significant gaps with respect to where federal jurisdiction can apply and where provincial jurisdiction already applies.

The Chair: You're out of time. Thank you, Mr. Perkins.

I'll now turn to Madam Lapointe for six minutes.

[*Translation*]

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

Ms. Gratton, with this bill, will Canada's legislation be in step with international privacy rules and standards, especially the GDPR in the EU?

Ms. Éloïse Gratton: I think the bill is acceptable in that it really seeks to balance privacy protection and the interests of organizations that collect personal information for legitimate purposes. That said, the bill doesn't go as far as Europe's regulation, which is clearly more robust in a number of ways.

● (1605)

Ms. Viviane Lapointe: Previously, you had this to say about Canada's first privacy laws:

> Forty years later, this concept remains one of the dominant theories of privacy and the basis for privacy protection laws around the world, including [even our bill]. The “notice and choice” approach these laws impose is no longer realistic: individuals are overloaded with information in quantities that they cannot realistically be expected to process or comprehend.

The bill as drafted helps to foster the realization that privacy protection can no longer be the responsibility of individuals. Technology has advanced so much that the average person could never completely protect their privacy and information online. Do you think the bill adequately protects personal information by requiring corporations and businesses to assume responsibility for privacy violations?

Ms. Éloïse Gratton: I should probably start by clarifying that statement.

One of the underlying principles of privacy is that individuals retain control over their personal information. That idea goes back to the early 1970s, before the Internet came along. Things have obviously changed since then. Today, we are dealing with huge amounts of information and complex business models, not to mention partnerships. On top of that, privacy policies are very long, complex and detailed to ensure that individuals have all the information. However, they don't take the time to read all that information because it's so complex and burdensome.

Keeping that in mind, I think it's worthwhile to try to reduce the need for consent and to focus on situations that require the individual's consent, while introducing other legal grounds for protecting the individual, a bit like what Europe did with the GDPR. In that respect, with the exceptions to consent, I think the bill is definitely a step in the right direction.

Clearly, other safeguards are needed. For instance, in order for the legitimate interest exception to apply, the company has to document why it considers the collection or use of the information acceptable and carry out a risk assessment. There are safeguards. Companies have to do a bit more work to make sure that they are protecting individuals' right, and they are subject to penalties. Companies want to be compliant and good corporate citizens, of course, but they also want to avoid penalties. With the penalties, which are in line with what we see in Europe, the bill provides that incentive.

Ms. Viviane Lapointe: Could you give us your opinion on the measures that Bill C-27 provides in terms of data protection?

Ms. Éloïse Gratton: Are you talking about security?

Ms. Viviane Lapointe: Yes, that's right.

Ms. Éloïse Gratton: There aren't that many changes, in the sense that the article dealing with protection and adequate security measures will still be technology-neutral. We're referring to current standards. As lawyers practising in this field, we will often rely on decisions handed down by privacy commissioners, who will cite the type of measures that were expected to be in place at the time, in the context and according to the given technology. I think it's right to keep that flexibility, to make sure we're relying on the security standards of the day, which are constantly evolving.

Ms. Viviane Lapointe: Thank you.

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

Mr. Lemire, you now have the floor for six minutes.

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

I thank the witnesses for their statements.

Ms. Gratton, even though clause 75 of the bill includes a prohibition on the use of de-identified information to identify an individual, clause 39 will allow companies to disclose an individual's personal information without his or her knowledge or consent for socially beneficial purposes to organizations that are not subject to the law. How can we strike a balance between protecting personal information and facilitating this disclosure, especially when unregulated organizations are involved?

● (1610)

Ms. Éloïse Gratton: At the moment, clause 39 introduces an exception, but it goes in one direction only. Private sector companies can share information without restriction, but with public sector bodies. In my submission, I point this out and say that there should be protections in place, even if they are public sector bodies. My reasoning is that if it's good for the public sector, maybe it's also acceptable between private sector companies.

Obviously, there have to be security measures. For example, in Quebec, there may be exchanges in certain cases. You have to do a privacy risk assessment first, and then you have to file an agreement that has to include certain clauses. In my opinion, there's a way to strike a balance.

However, I think excluding private sector companies from the application of clause 39 here is shooting ourselves in the foot. Private sector companies have a lot of resources, ideas and data. Why deprive ourselves of this if we want to favour innovation?

Mr. Sébastien Lemire: There may be a loophole here, but what additional safeguards or measures should be put in place to ensure more responsible data exchange in such a case?

Ms. Éloïse Gratton: As I told you, there could be a privacy impact assessment. Risks would be identified and how to reduce them. Organizations wishing to exchange data could be required to provide this assessment to the Office of the Privacy Commissioner of Canada, allowing oversight of projects where data is exchanged. These organizations could also be required to enter into contracts that include minimum requirements for the implementation of security measures.

If we notify the commissioner, assess the risks, provide contractual clauses and ensure that data is properly secured and de-identified in certain situations, I think we could strike an acceptable balance.

Mr. Sébastien Lemire: In another connection, Bill C-27 obviously raises the issue of the precedence of Quebec's recently updated private sector privacy legislation. As you know, Minister Champagne has made public a letter he sent to members of our committee to clarify the federal government's position in this regard. He acknowledges that the provisions of the Quebec legislation are essentially similar to those of the federal bill, and that they can take precedence. Do you agree with this analysis?

Ms. Éloïse Gratton: The Quebec and federal provisions are certainly similar. Those in Quebec are probably a little more stringent in some respects and include additional requirements, such as profiling in section 8.1 of the Quebec law, as well as the need to perform risk factor assessments before transferring data outside Quebec.

The analysis you mention is therefore certainly acceptable: if we compare the new Quebec requirements with the provisions of Bill C-27, there is no doubt in my mind that Quebec would pass the test.

Mr. Sébastien Lemire: Thank you very much.

Mr. Therrien, Bill C-27 emphasizes the need for informed consent by devoting an entire section to it. However, we have seen the rise of platforms favouring the use of opt-out formulas. These are the famous opt-out rather than opt-in options. In your opinion, does this bill do enough to protect users of digital platforms from the pitfalls of these opt-out formulas?

Mr. Daniel Therrien: I was telling Mr. Perkins that clause 15 of Bill C-27 will probably need to be amended. Section 6.1 of the current act sets out certain requirements for consent to be considered valid, including the notion that the person giving consent must be able to understand the purposes and consequences of disclosing the information. This terminology does not exist in Bill C-27 and I believe it would be much better to retain the current wording.

Mr. Sébastien Lemire: In a conference I heard you speak at recently, one of the things you talked about was personal information as a raw material, whether it's public or personal. I think it's worth thinking about this question in committee. Does information that is posted on Facebook, for example a photo, really become public?

● (1615)

Mr. Daniel Therrien: In common parlance, when people post personal information on a social media platform and allow certain other people to see it, one might think that this information becomes public. Importantly in this context, one might also think that companies and commercial organizations could use this information as public, rather than personal, information. However, the current law provides that this information remains personal and cannot be used by companies, except in accordance with the law.

I think this is a good aspect of the current law, and the fact that nothing in the current text of Bill C-27 changes this is a good thing.

Mr. Sébastien Lemire: Thank you.

The Chair: Thank you, Mr. Lemire.

Mr. Masse, you have the floor.

[*English*]

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

Maybe I'll start with the witnesses who are online.

I'd like to get everybody's position on the tribunal—whether you're in favour or opposed, and a couple of thoughts on that. I'll have to share the time with everybody, but we'll start with our online witnesses, because they often get missed.

Please, who wants to go first? Pick yourselves.

Ms. Éloïse Gratton: I'll start, if that's okay.

The Privacy Commissioner's office has been working so far as an ombudsman model, and it also has an advisory branch. That's quite useful.

This means that when there's an investigation, there's a conversation. There's a dialogue. In some cases, businesses can go knocking on their door and say: "Hey, what do you think about this business model? We want your input." I'm just concerned that if there's a tribunal, will that relationship potentially be impacted? I guess that's concern number one.

My other concern is the fact that a lot of these privacy principles are quite flexible, and we need that in our privacy law. On the notion of consent, sometimes it's expressed and sometimes it's implied. It's subject to the reasonable expectation of the individual. Security measures have to be adequate in light of the content. There is so much in grey zones and uncertainty. Now it's in the law. It's no longer principles. Adding the tribunal is just perhaps a layer of risk for businesses that have to navigate with a lot of grey zones in the law.

Mr. Brian Masse: I have only about four minutes or so left. If we could share, that would be great.

Dr. Khaled El Emam: I'll just add one quick point: Reducing uncertainty is always beneficial. To the extent that any additional requirements increase uncertainty or add additional hoops for organizations to know what they have to do, it generally results, in some places, in paralysis or important decisions not being made.

Mr. Brian Masse: Mr. Fraser is next. I'm going across the board here.

Mr. David Fraser: Starting with the assumption of having order-making powers and penalties, we do need to have an independent decision-maker, in my view. That could be the tribunal or that could be the Federal Court.

I don't see why it couldn't be the Federal Court. I'm concerned that standing up a tribunal is actually going to delay the implementation of this legislation, because it's going to take a number of years simply to hire the staff, rent the photocopiers and all of those other things.

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

Next is Mr. Therrien.

Mr. Daniel Therrien: I will try to be brief.

The goal of these provisions should provide quick and effective remedies for citizens. In no other jurisdiction that I know of is there a tribunal such as that proposed in this legislation. In all other privacy jurisdictions, the original decision-maker, including with the power to make orders and set fines, is the data protection authority that is the equivalent of the Office of the Privacy Commissioner.

I hear concerns about the difficulty for the OPC to work with different roles. That is not a problem in other jurisdictions. It is well known in law that it is possible for an administrative tribunal to have investigative, advisory and adjudicative functions. This needs to be managed and it can be managed. There is no problem there.

I think the tribunal will create delays and will simply be duplicative of the expert work of the Office of the Privacy Commissioner. Again, there is no precedent internationally for this.

● (1620)

Mr. Brian Masse: Mr. Kardash, I don't know if I have time.

You can take it from my next round, Mr. Chair. I would like to hear him.

Thank you.

Mr. Adam Kardash: I personally am fully in favour of the tribunal.

I think it's important to start the conversation with looking at the sheer quantum of the potential penalties for contravention of the act, which, comparatively speaking with any other statutory framework, is a mess. With larger corporations, it's hundreds of millions of dollars.

As Mr. Fraser mentioned in his opening remarks, it's absolutely imperative in a circumstance when you're introducing a regime with that level of penalty, which could be potentially impactful for businesses in every constituency here, that you just have a procedural fairness piece on that and that everyone agrees with that. This will add to that procedural fairness piece and it will allow for, in my view, an appropriate articulation of whatever the penalty is or should be in a particular circumstance.

Mr. Brian Masse: Thank you.

Thank you, Mr. Chair.

Thank you to the witnesses.

The Chair: Thank you very much.

I will now turn to Mr. Williams for five minutes.

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

Mr. Kardash, I'll start with you.

I know it's all in here, but can you explain, in one sentence for each, what the definition of "de-identify" is and what the definition of "anonymize" is?

Mr. Adam Kardash: It's a good question. These are technical terms, and they often cause confusion.

CANON was established to help demystify this terminology, because that ambiguity creates uncertainty and uncertainty creates reticence risk. It's an issue.

Simply put, de-identifying data is the removal of direct identifiers. The language is quite elegant within current language in the CPPA. When you remove direct identifiers, you still have indirect identifiers. In other words, the data is still potentially identifiable. De-identified data is still regulated by the statutory framework.

Anonymized data, which was the subject of my opening remarks, has a more exact definition that sets the standard for the application of the statute. I think it's really important to go through, given how technical these terms are. The current definition talks about irreversible and permanent modification in accordance with generally accepted best practices to ensure that an individual cannot be identified from the information, directly or indirectly.

Our view and the view supported by our extensive consultations and jurisdictional analysis, etc., is that it doesn't work. You need the contextual piece of the reasonably foreseeable risk in the circumstances, which is embedded in Law 25 and which is embedded in PHIPA. You'll see in the briefs that we provide you with these other regimes.

Anonymized data means there's no foreseeable risk, in the circumstances, to identify the individual.

Mr. Ryan Williams: If I understand you correctly, you've stated that you can use de-identified information as long as it complies with clause 74 of the bill, as you've noted here. Is that correct?

Mr. Adam Kardash: Yes, the essence is.... It's even broader than that. I think it's important to note that de-identified information is subject to all the protections within the statute.

Yes, there has to be a recognition of how you de-identify. I think you're referring to clause 74 with proportionality, and it has to be brought in. That's right.

Mr. Ryan Williams: The reason I say that is there is a case study we can use. Mr. Therrien knows well about this.

In the holiday season of 2021, Telus was selling data to the Public Health Agency of Canada. Canadians who went out during a lockdown to visit the pharmacy or went to the grocery store were tracked, and that data was sold to the Canadian government.

We did then talk about this in the ethics committee.

Mr. Therrien, you were very succinct in your comments. There were two parts to this. There was not implied consent. You noted, “While there is reference to 'data for good' programs somewhere in the Telus privacy policies, while the government does make an effort to inform citizens...I do not think anyone would seriously argue that most users knew how their data would be used.”

I'm trying to back this up. My real question is, does this act, with your amendments, fix that situation?

I'm going to ask Mr. Kardash that first.

Mr. Therrien, the question for you afterwards would be this: Does this act go far enough to address the consent model we're looking for if this were to ever happen again?

Mr. Kardash, I'll start with you.

Mr. Adam Kardash: The requirements for consent in the regime apply to personal information. It could be de-identified data, which is just the removal of direct identifiers. They don't apply to personal information where, as the statute is currently drafted, it's “reasonably foreseeable”.

The Office of the Privacy Commissioner of Canada did an excellent job in that investigation. I know it well; I acted in that investigation. In their careful analysis, they determined that the data that was received by the Public Health Agency of Canada was not identifiable in the context of the disclosures that took place. Therefore, if the data was not identifiable, it's not personal information. If it's not personal information, it wouldn't be subject to the consent requirements or to the statutory regime.

Our surgical amendments make no difference to that. In fact, it reflects the current law, etc.

Again, I can't overstate the exceptionally high standard for what is personal information right now. You have to look contextually at the circumstances and you have to look at the technical methods for de-identifying, which are wrapped in administrative controls, security controls and physical controls. That suite of controls was implemented on top of some very sophisticated methods to ensure that the Public Health Agency of Canada, as determined by the Office of the Privacy Commissioner of Canada, did not receive any identifiable data.

● (1625)

Mr. Ryan Williams: Thank you.

I want to allow some time for Mr. Therrien.

Sorry; I only have a couple seconds left.

Mr. Daniel Therrien: I would agree in large part with Mr. Kardash.

When I was commissioner and we were seized with this matter, we had not seen the measures taken by companies to anonymize the information. In short, de-identified information is still personal information and requires consent.

Do the consent provisions need to be improved in the CPPA? Yes, they do, but that's in the scenario of de-identified information. If the information is truly anonymized, it is no longer personal. It is no longer at risk and can be shared more freely.

Mr. Ryan Williams: Thank you.

[*Translation*]

The Chair: Thank you very much.

Mr. Turnbull, you have the floor.

[*English*]

Mr. Ryan Turnbull (Whitby, Lib.): Thank you, Mr. Chair.

What a great discussion we're having today. I really thank you all for your expert testimony.

Maybe just to follow up on Mr. Williams' line of questioning, Mr. Kardash, I'll point a couple of questions toward you.

Just so I understand correctly, you've said that basically the current definition of anonymized data is too high a standard. It doesn't align with other statutes. You're saying that essentially the standard is already high enough within those other statutes and we should just harmonize the CPPA with that.

Is that correct?

Mr. Adam Kardash: Yes. It's interoperability. I'll give three very quick components. I do recognize the time constraints.

Number one, it's a very high standard as articulated by jurisprudence. Number two, we cite at least 12 statutes in there for you to look at off-line, including Law 25 and a very rigorous regime, the Personal Health Information Protection Act, that basically incorporate this contextual requirement, "reasonably foreseeable risk in the circumstances", or very similar wording.

It's for interoperability, which is absolutely critical; that's right.

Mr. Ryan Turnbull: Got it. Great.

You used the term "expressly contemplates contextual risk", which I'm not sure I fully understand. Could you explain that a little bit further?

Mr. Adam Kardash: Yes. I would ask if my colleague Khaled could also supplement my comments.

Mr. Ryan Turnbull: Sure.

Mr. Adam Kardash: When you are looking at a particular record of data, you have to look at it in context in order to make a determination. Doing that is actually for privacy protection. "Reasonably foreseeable in the circumstances" is that contextual factor that needs to be articulated. It's consistent with best practices. This is the way in which risk management is implemented for the purposes of this analysis.

Khaled, I would ask you to please supplement that. You deal with this so practically. It would be very helpful.

Dr. Khaled El Emam: I think the key point is that the anonymized data includes modifications to the data as well as the additional controls that the data user or data recipient has to put in place—additional security controls, privacy controls and contractual controls. It's not just about the data; it's about the additional controls.

These are contextual in the sense that, depending on the sensitivity of the data, you may implement more controls, for example. It's not just about the data; it's about the data and the context around it, or the additional administrative and technical controls around it.

Mr. Ryan Turnbull: Thank you for that.

Ms. Gratton, Mr. Therrien said that the European law is the gold standard. He talked about how there is no real inconsistency in terms of protecting privacy and the legitimate interests that you had rightly pointed out. I think you were making very specific suggestions regarding the different types of legitimate interests that are included currently in the CPPA.

Would your suggestions actually further align us with the European law or the gold standard that Mr. Therrien mentioned?

● (1630)

Ms. Éloïse Gratton: I think so too. In fact, you'll note from my brief that I'm actually proposing that the "legitimate interest" consent exception be more aligned with the GDPR.

Mr. Ryan Turnbull: Okay. Great.

Are there any places where you think we could go, or need to go, further than the European law?

Ms. Éloïse Gratton: I don't think we need to go further than the European law. I guess my other comments really have to do with making sure that we're not hampering innovation.

Mr. Ryan Turnbull: Yes. I see the point that this is really about a balancing act. I think everybody has talked about that. It's how to get that balance right.

We started off our last meeting with the current Privacy Commissioner by having that discussion as well. We sort of got to that point at the end, that this is a delicate balancing act. I know that some members have expressed points of view that may side a little bit more with perhaps weighting privacy rights and protection even more. I think we've also heard witness testimony that innovation and privacy rights are largely aligned in many of the cases.

Ms. Gratton, from your perspective, is there a risk that we could go too far? I take it that a lot of your testimony is related to where we draw the line and how we can facilitate a process whereby innovators can continue to innovate and offer the value of all the digital tools that enhance our lives and that I think we all benefit from on a daily basis.

Could you speak to that?

Ms. Éloïse Gratton: When you say "go too far", I'm assuming you're talking about protecting privacy—

Mr. Ryan Turnbull: I mean stifling innovation, because I'm concerned with just getting the balance right on both sides of this. I obviously value my fundamental right to privacy, as all Canadians do. At the same time, I don't want to stifle innovation and the kinds of benefits that Canadians get from these digital tools.

Ms. Éloïse Gratton: What I can say is that of the four recommendations I'm getting, three out of four are actually proposing that our law be more aligned with the laws of Europe or Quebec, which are actually more stringent.

It's also an issue with interoperability and making sure that our requirements are harmonized, especially when they make sense. We don't need to reinvent the wheel. If Quebec got it right, and if in Europe they got it right through the GDPR, why are we reinventing the wheel?

Perhaps one issue I'd like to raise is that in Europe they had interpreted their requirement to mean websites need cookie banners, and five years later they're reassessing that. There's a movement in Europe, the cookie pledge, and they are reassessing whether they are better protecting website users with these cookie banners, which are extremely complex. People are just accepting them.

I think maybe one lesson learned from Europe that we should not replicate here is pushing for website cookie banners.

The Chair: Thank you very much, Madam Gratton and Mr. Turnbull.

Mr. Lemieux is next.

[*Translation*]

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

Mr. Kardash, the Canadian Anonymization Network has a particularly interesting case. According to a paper you published in May 2023, the current definition of “anonymize” sets an extremely high and virtually unattainable threshold for circumstances under which it can be concluded that information can no longer be used to identify someone.

The document refers to Bill 25, adopted by the Quebec National Assembly in 2021. The latter uses more moderate language, to ensure that anonymization is achievable, and advocates the adoption of similar language in order to ensure interoperability between the two regimes.

In your opinion, if the language is left as it is in the current bill, what will be the implications for Quebec companies, particularly small and medium-sized businesses that will be subject to Bill 25, since it would take precedence, but also to this bill, if their operations cross the border?

[*English*]

Mr. Adam Kardash: May I ask for clarification? Are you asking what the impact would be if we do or we do not make our recommended change to the definition of “anonymize”?

I'm sorry. I just want to clarify so that I answer your question correctly.

[*Translation*]

Mr. Sébastien Lemire: I find your perspective interesting, but I'd like you to talk about what will happen if we apply it and if, on the contrary, we don't apply it.

● (1635)

[*English*]

Mr. Adam Kardash: Okay. It is really important for companies to have legislative schemes in the privacy area that are interoperable. If you don't have interoperability, you'll create lots of confusion, lots of uncertainty. There will be reticence risk, which is the risk of not doing anything, and just overall problems with it.

All we're doing is actually incorporating a well-understood concept to ensure the term was used in a harmonized way and interoperabilities were similar. It's really important to do that. There would be adverse consequences: If you don't put it in, there will be an open question of why. Obviously it's a different standard, and our view is that there's no need for that. Privacy protection could be there. It's a very high standard right now, and we just don't need that at all. It will not be beneficial at all. Especially, striking the balance that we just heard from before.... That's why we're so strongly in support.

I will add that we had these consultations. They were extensive. A working group spent countless hours dealing with it. We met with folks. This was universally accepted in all our discussions. Yes, let's make it clear. Let's stay with this. It's the appropriate and prudent approach to take.

[*Translation*]

Mr. Sébastien Lemire: Thank you very much.

The Chair: Thank you.

Mr. Masse, the floor is yours.

[*English*]

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

I apologize for my leaving off and on during the meeting. There are world events that particularly complicate my riding in Windsor and the Detroit region. I apologize if I repeat something or miss something, but I will go back and listen to the rest of the stuff I've missed from the witnesses.

Mr. Therrien, I do want to ask a question about a certain situation. The Competition Bureau recently had to pay a fine for investigating the Shaw takeover by Rogers and opposing it; and it ruled against them. Through other testimony we learned it might be the same process that could happen here for the privacy commission in this legislation. We have to sort that out, because I was told something from one, and we had different testimony from another.

Again, with the tribunal, I know you have a little more to offer. On creating this type of a body, do you really think it could undermine the strength of the privacy commission in general? I worry about that, because I know that the United States doesn't have this model; but for ourselves, it has actually served Canadians quite well.

I'd like you to expand on the vulnerability if we change the route that we have right now.

Mr. Daniel Therrien: Thank you for that.

I think there is a risk of the OPC being undermined—in the following way, at least. The federal office works—and has to, because data flows internationally and within provinces in Canada—with colleagues in Canada and internationally.

As I explained in my earlier answer, there is no other jurisdiction with the type of tribunal that is proposed federally under the CPPA. That would put the OPC in a situation such that when it conducts joint investigations with colleagues across Canada or internationally, its position would be effective later than that of its colleagues. The OPC would then have to wait for the blessing of the tribunal for an order to be upheld or for a penalty to be imposed. That's one thing.

However, even more importantly, Canadian citizens would have to wait longer than others in other jurisdictions, including in Quebec. The CAI in Quebec has order-making and fine-imposing powers. There's a difference in the rapidity with which Canadian citizens would have protection compared to other jurisdictions.

Mr. Brian Masse: Thank you.

Thank you, Mr. Chair.

[*Translation*]

The Chair: Thank you very much.

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

[*English*]

Mr. Brad Vis: Thank you to all of the colleagues for your expertise on this very important bill.

I'm very concerned about children. If you watched my testimony in the last meeting, I'm very concerned about how a child can consent to provide any sort of data that could be used by a business interest.

This is an open-ended question to anyone who wants to respond. Under “Socially beneficial purposes”, how do we define a socially beneficial purpose? It's in the act, in proposed section 39.

● (1640)

Mr. Daniel Therrien: I think you're talking about the context of children.

Mr. Brad Vis: Yes.

Mr. Daniel Therrien: If we look at proposed section 39 and the definition of socially beneficial purposes, one of these purposes would be for disclosure to “a health care institution, post-secondary educational institution or public library”.

Certainly, health care—

Mr. Brad Vis: Thank you.

I'm most concerned about proposed paragraph 39(1)(iv), which is “any other prescribed entity”. What's a prescribed entity in the context of a socially beneficial purpose as it could relate to de-anonymized data from a child?

Mr. Daniel Therrien: That would be a good question for the government, because there has been no regulation.

Mr. Brad Vis: Okay. That answers my question. We don't know.

What I hear from you today is.... We're talking about consent as well. My concern is the consent of a child. We don't have a definitive age for a minor in this legislation.

Do any of you want to comment on whether we need to define the age of a child, and whether there should be different tiers of consent related to a minor in this legislation?

Again, it all goes back to my kid on an iPad, when I'm sitting on an airplane or driving somewhere. He's in the back and he's clicking on certain things. I don't know where that information's going, and I get scared about that. I'm fearful as a parent. I know every committee member around here has similar concerns.

How can we address that in this legislation to make sure that children are protected?

Mr. David Fraser: I'm happy to weigh in on this subject with some thoughts, because it's something I have turned my mind to.

In the legislation, it refers to minors, and minors are defined by provincial law. Minors are 18 in Alberta and Quebec and 19 everywhere else, so there's a different line.

One of the challenges that I think exist with children and privacy is that there really are no easily drawn bright lines that say that under this particular magic age, you are completely under the control of your parents and you have no ability to consent in a valid, true way—

Mr. Brad Vis: Exactly.

Mr. David Fraser: —or over this age, you're magically endowed with those particular powers.

As a parent of three young men now, I know that you can tell that at different ages there are different levels of maturity, and it's difficult to determine. The way that it works in practice is difficult to operationalize. You have to take into account the individual characteristics of the young person, and whether they are able to....

Mr. David Fraser: Mr. Therrien talked about the requirements for knowledgeable, informed consent. Is the child capable of understanding what it is they're consenting to and what the consequences are? It's actually tied pretty similarly to consent to medical treatment, so it's not completely isolated in its own little world.

Mr. Brad Vis: I'm going to pass it over to Mr. Kardash. That was a great point.

Mr. Adam Kardash: The statute expressly sets out that minors' data is sensitive information. It's expressly contemplated in there.

Mr. Brad Vis: Yes.

Mr. Adam Kardash: In doing so, what ends up happening is that many of the other provisions in the statute have to look at the treatment of sensitive information. For instance, when you're dealing with safeguarding, safeguarding is implemented appropriately to the sensitivity.

When you consider different requirements—

Mr. Brad Vis: Thank you.

Would the provisions related to sensitive information outlined in proposed section 12 override, say, proposed section 38 of the consumer privacy protection act as it relates to the use of information for literary purposes, for example, in the context of children?

Mr. Adam Kardash: Once you take data, and there's more sensitivity to it, there will be a holistic set of provisions in the act that will be applied. Even currently, the case right now with subsection 5(3) of the Personal Information Protection and Electronic Documents Act—and it's amended now and is even more involved—is that organizations are only allowed to collect, use and disclose personal information that a reasonable person would consider appropriate. That might seem broad, but that's privacy protective in nature because the sensitivity of the data will impact your statutory analysis of what a reasonable person would consider appropriate in the circumstances.

Mr. Brad Vis: Do we need to define a “child” in this legislation?

● (1645)

Mr. Adam Kardash: I don't think so. Minors under the age of 13 wouldn't have the capacity to consent. That would be protected. Data would be protected otherwise.

There is an idea about specifying “under the age of 18”. It works right now. I don't think you have to do it.

The key thing in the statute, which goes to the heart of your concern.... I think the concern of everyone in the room, certainly myself, is that the protection of minors is very important, but there's express contemplation already in the statutory framework that this is sensitive data, and that has a flow-through impact and would be treated well, certainly from a statutory interpretation perspective.

Mr. Brad Vis: Mr. Therrien, do you believe we need to do more to amend proposed section12 to be 100% sure that the rights of children, when we define a fundamental right to privacy, are given the attention they deserve?

Mr. Daniel Therrien: Minister Champagne has tabled amendments to the preamble and to proposed section 12 that would provide greater protection to children. Again, that is a step in the right direction, but I'm concerned that the terminology used may be too limitative, and that is why I have recommended in the text I provided to you that proposed section 12 be amended to refer to the concept of “the best interest of the child”. That concept has to be interpreted contextually. It is not limited.... Again, the language proposed is a step in the right direction, but it may be too limitative, and I think the concept of “the best interest of the child” would provide fuller protection.

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

[*Translation*]

The Chair: Thank you very much.

Mr. Gaheer, you have the floor.

[*English*]

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

I just want to say thank you to the witnesses for appearing before the committee and for their useful testimony.

My questions are playing off what Mr. Vis said. I wanted to talk about socially beneficial purpose as well. My questions are for Mr. Kardash.

We know that according to proposed section 39 of the consumer privacy protection act, an organization has the right to disclose to certain entities de-identified personal information without the knowledge or the consent of the individual if the disclosure is made for a socially beneficial purpose. That is defined in the bill. It means “related to health, the provision or improvement of public amenities or infrastructure, the protection of the environment or any other prescribed purpose.”

Do you think that this definition of “socially beneficial purpose” is enough to protect the privacy interests of Canadians, in addition to the fact that this is already de-identified information, which, as you said in your opening testimony, is already a pretty high bar? It's an exacting standard.

Mr. Adam Kardash: This provision was the subject of extensive discussion in CANON's consultations. In our brief, which was submitted to INDU, you'll see some specific provisions we are suggesting to enhance privacy protection with respect to the personal information that would be subject to these disclosures. Éloïse Gratton mentioned elements of these.

We indicated, in addition to personal information being de-identified, notification to the Office of the Privacy Commissioner of Canada and entering into a specific agreement that binds the recipient. Then we added—in order to ensure we stay temporal with this and current—that the organization must comply with any other prescribed requirement. It gives the government an opportunity to reassess and then introduce regulations to further add even more requirements for perhaps the recipients of the data or the disclosing entity.

We think disclosure for socially beneficial purposes is excellent, because of the good. It's “data for good”. However, we strongly believe, and we've made specific recommendations to this end, that there should be additional privacy protections implemented with respect to that provision in order to help strike this balance.

Mr. Iqwinder Gaheer: When I hear that testimony.... You said you have already identified that it's a pretty high standard, an exacting standard. You actually want to lower that bar for information that's de-identified and that can also serve a socially beneficial purpose.

Do you feel that strikes a balance already, or would you go even further?

Mr. Adam Kardash: Our sense—again, this is based on extensive consultations—is that, as the bill is drafted, and taking into account that you can't look at any exception to consent in a vacuum, all of those disclosures are subject to many statutory provisions in the act, if you are relying on an exception to consent to disclosure. However, with respect to this provision, we believe it would strike the necessary balance if you enhance the privacy protections with our suggested amendments, together with—as mentioned by other witnesses in today's hearing—a prescribed requirement for additional protections over time being introduced by the government, if it feels it's necessary to do so.

“Data for good” is something that could be extraordinarily helpful. There's a wealth of unknown benefits to all Canadians. When we saw this provision initially, there was broad-based support. However, we fully recognize some of the concerns, and we address them with our suggested revisions. We think that with our suggested revisions, it's a good balance.

● (1650)

Mr. Iqwinder Gaheer: Thank you. I support your proposals. I just wanted the testimony to come out.

My other question is regarding disclosure of personal information without the knowledge or consent of the individual, if it's made for a business activity.

That definition is also given, where “(a) a reasonable person would expect the collection or use for such an activity” and “(b) the personal information is not collected or used for the purpose of influencing the individual's behaviour”.

What do you think about this definition and how it's being narrowed?

Mr. Adam Kardash: I welcome others to comment.

My sense is that the government did an excellent job articulating some circumstances in which it's expected organizations would be using the data. These are not particularly controversial types of uses. Again, it's just exception to consent. It doesn't mean you're not subject to all the other requirements that are applicable in the circumstances. I think that's something often overlooked in the discussion.

Our careful review of that is.... Those were welcomed, and the government did an excellent job with them.

Mr. Iqwinder Gaheer: Thank you.

[*Translation*]

The Chair: Thank you very much.

Monsieur Généreux, you have the floor.

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

I also thank the witnesses.

Mr. Therrien, you were the Privacy Commissioner when former bill C-11 was tabled. You had proposed amendments and stated that the bill was a step backwards from what existed at the time.

Your successor proposed 15 amendments, which you say you agree with. However, the government only retained five of them. Of the 10 it did not keep, which ones do you think should fundamentally be included in the current bill?

Mr. Daniel Therrien: The recommendations are all important, and I presented others in my brief, particularly on the issue of proactive audits. If I had to pick just one, I'd choose the obligation to carry out a risk assessment, which I think should become a legal requirement.

There's also another point, which is less often discussed. In the current bill, organizations would have very wide latitude in defining the purposes for which they can use personal information. As I did when I was commissioner, Commissioner Dufresne recommended that the purposes for which information can be used be explicit and precise. These words are important. At present, companies can define these purposes pretty much as they please. Forcing them to define these purposes a little more narrowly would be one way of ensuring a better balance. Moreover, such a provision would be in line with European legislation.

Mr. Bernard Généreux: Earlier, Mr. Fraser said that, in his view, the tribunal should be an independent body of the commissioner's office, not an internal body managed or promoted by the commissioner under the law. What is the fundamental difference? I understand there are two visions in relation to this: Mr. Fraser wants the tribunal to be completely separate from the commissioner's office, but I think you're suggesting that the tribunal should be an internal body of it.

If we give broad powers to the commissioner so that he's both judge and party, promoting the right to privacy, and also deciding disputes under the bill, isn't there a risk that he'll be put in a conflict of interest situation?

● (1655)

Mr. Daniel Therrien: It's a possibility, but I wouldn't call it a risk. It's a possibility that the law routinely provides for, incidentally. There are a large number of administrative tribunals that are capable of conducting investigations and providing advice as well as having adjudicative powers. Obviously, these powers must be kept separate within the organization. The same would be true if the Office of the Privacy Commissioner of Canada had these powers without a tribunal. The decision, for example an order made by the Office of the Privacy Commissioner, must be subject to judicial review to ensure that it has been fair to business. Often, this kind of potential conflict is handled smoothly by administrative tribunals.

Mr. Bernard Généreux: Mr. Fraser, do you have anything to add?

[*English*]

Mr. David Fraser: Certainly I agree that it's two different models. We also have, for example, a human rights commission and a human rights tribunal, a competition commissioner and a competition tribunal. There are other scenarios in Canada in which that particular model is applicable. There is the possibility for conflicts, and one would have to have controls and procedural safeguards within the Office of the Privacy Commissioner of Canada to make sure that those conflicts did not arise.

Given the stakes that this legislation presents, with multi-million-dollar penalties, even multi-billion-dollar penalties when you look at percentage of a company's global turnover, it raises the requirement for additional procedural safeguards. You can think of it as a scenario in which a police officer can write a ticket, and you could pay the ticket and plead guilty and go on your way, or you can dispute it, and the police officer has the burden of proving in front of an impartial decision-maker whether or not the facts alleged in that ticket are borne out. That would be the model that I would advocate.

Otherwise, maybe we can split the difference, and when it comes to anything that has a significant penalty over a certain threshold, it would require those additional safeguards. Those are going to be important.

I would also note that we're seeing more and more multi-jurisdictional investigations taking place simultaneously, so organizations are going to be subject to multiple penalties in multiple places arising from the exact same investigation. The fine threshold in Quebec is similar to the fine threshold here. You could find those to be doubly levelled, which again, at least to me, raises the stakes higher.

[*Translation*]

Mr. Bernard Généreux: Mr. Therrien, I don't want you to quarrel, but what do you think of his answer?

Mr. Daniel Therrien: It's obvious that the penalties provided for in the law are extremely significant. This is also the case in Europe and other countries, as well as in Quebec with Bill 25. In all these models, without exception, the court of first instance, the equivalent of the privacy commissioner's office, is able to make these rulings.

As I was saying to Mr. Masse, if the federal office doesn't have the same tools as its counterparts, it risks creating significant complexities in joint investigations with other jurisdictions.

The Chair: Thank you very much.

[*English*]

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

Mr. Tony Van Bynen (Newmarket—Aurora, Lib.): I am wondering if this legislation reflects the current state that we're in. For example, if we were 10 years back, with the legislation we're proposing now, would we be in a different situation? I'm thinking of Facebook, ChatGPT and social media.

Anyone who doesn't think their privacy already has an intrusion doesn't have a cellphone or a social media account. How can we change that, or is the intent to control that? How can we best do that?

I'll start with Mr. Fraser.

Mr. David Fraser: I guess I would start with wondering whether you think that we should have a world without Facebook, ChatGPT and things like that.

In my view, this legislation takes what we have existing in PIPEDA and largely, as I said, turns it up to 11, so it puts a greater requirement of diligence on the part of organizations in order to, for example, justify their decision-making, document risks and do those sorts of things, and then it has those substantial penalties.

Had this been implemented 10 years ago, I'm not sure that the universe would be all that different, because I think it's still based on the 10 principles from the Canadian Standards Association's code for the protection of personal information, which are very Canadian principles with respect to privacy.

I am very curious to hear from Mr. Therrien in terms of how he thinks it would have been different had he entered office with the CPPA at his disposal.

● (1700)

Mr. Tony Van Bynen: Go ahead, Mr. Therrien.

Mr. Daniel Therrien: I think that the CPPA brings us much closer to where we ought to be in 2023. With the new implementation of artificial intelligence, part 2 of Bill C-27 is an attempt to align Canada's legislation to that new technology.

There's no perfect solution in all of these situations. There are people who think that the artificial intelligence act is so skeletal as to be meaningless, and there's some merit to this. I think it's okay for where we are today.

One virtue of the legislation before you is that it continues with the consent model in many circumstances in which consent can possibly be given, but it also recognizes that there are important limits to the consent model, such as legitimate interests and socially beneficial purposes, but I think the missing piece is that these additional flexibilities that reflect the current use of technology have to be implemented within a rights protection framework.

Although the minister's latest amendments bring us a bit closer, we are still quite a way from where we ought to be, and that is why I recommended that proposed sections 12 and 94 on penalties, particularly on penalties, are important, because what's the value of having a recognition of privacy as a fundamental right if there is no penalty when you breach that principle?

Mr. Tony Van Bynen: Do you think that what we're introducing now is going to change the behaviour and uses of data currently in the hands of some of these organizations?

Mr. Daniel Therrien: I hope, with time, with not only penalties but including penalties, that it starts with companies acting responsibly and regulators working with businesses to ensure that the law is being implemented. There are advisory roles to the OPC that are important, but penalties should also be there so that the right set of incentives will be there for behaviour to change.

Mr. Tony Van Bynen: This comes back to your suggestion that there should be proactive audits by the Privacy Commissioner to ensure that whatever additional responsibilities are being created through this legislation are being adhered to.

Mr. Daniel Therrien: In brief, my point there is that it is extremely difficult, if not impossible, for individual consumers to understand how their data is used. It is even difficult for the regulator to understand how data is used.

How will violations be identified if we rely mostly on individual consumers to make complaints? There are provisions, I know, for commissioner-initiated complaints, but the model we have is premised mostly on the basis that individual consumers will complain.

In many situations, they don't know there's a violation. Proactive audits exist in other jurisdictions I've mentioned in my document, whereby the regulator can audit the practices of a company, not because there is belief that there's been a violation already but simply to reassure consumers that this new practice actually does comply with the law and therefore, yes, you can have confidence that it is privacy-protected, or no, it is not, and then the company will have to amend its practices.

I think proactivity is extremely important.

● (1705)

Mr. Tony Van Bynen: Thank you.

[*Translation*]

The Chair: Thank you very much, Mr. Van Bynen.

Mr. Lemire, the floor is yours.

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

Mr. Therrien, I would like to talk about subsection 4(a) and the right of children to exercise their own recourses, without a parent or a guardian. Should we consider going further on children's rights by recognizing the UN Convention on the Rights of the Child? Should children be given the right to exercise recourses and to be heard, either directly or through representatives, in any proceedings that concerns them?

Mr. Daniel Therrien: Part of the reason I am recommending that section 12 be amended to take into account the best interests of the child is because of the Convention on the Rights of the Child.

However, I am not an expert in Canadian constitutional law when it comes to the division of powers. What rights should a child have under the various proceedings? Is this something that can be done in federal legislation or is it more within the purview of provincial legislation? I wouldn't comment on that.

Mr. Sébastien Lemire: Would anyone like to comment?

Ms. Gratton, do you want to comment?

Ms. Éloïse Gratton: The discussion has evolved. What was your question?

Mr. Sébastien Lemire: In the context of the Convention on the Rights of the Child, should children be given the right to have access to recourses and complaint procedures and the right to be heard, particularly if they have experienced abuse or harmful situations?

Ms. Éloïse Gratton: Mr. Therrien is reluctant to speak because this involves the division of powers. Many of these issues fall under provincial jurisdiction. In Quebec, for example, the Civil Code governs the rights of the child.

I don't think those laws need to go beyond dealing with consent and protecting the data of children held by private sector organizations. That's really what these laws are designed to protect.

A little earlier, we talked about the age of consent. The bill could be more specific in some respects about the type of consent of the child, depending on their age. In Quebec, that distinction is made, but, again, in the rest of the world, it often varies. There is the age of majority and there are young children. Between the two, there are young people between the ages of 13 and 18 or 19, the age of majority.

In Quebec, the age of consent has been set at 14. This creates a lot of operational problems for organizations that want to put safeguards and measures in place to protect children. We should just keep that in mind.

Mr. Sébastien Lemire: Thank you very much.

[*English*]

The Chair: Thank you.

Mr. Masse, go ahead.

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

I want to touch on something we don't get a lot of questions on from this side, but I think it's important for you, Mr. Therrien, to highlight this.

For a political party, privacy laws apply in several jurisdictions, including Europe, British Columbia and now Quebec. The same should be true federally.

I would like you to expand on that point. It's something we don't seem to get a lot of questions on from this side of the table, but I think it is important to consider that potential.

Mr. Daniel Therrien: Again, interoperability was mentioned previously. There are laws in many other jurisdictions in Europe and within Canada—there's British Columbia and now Quebec—that provide that privacy laws actually do apply to political parties. That is a recognition of the fact that information held by political parties is almost always sensitive information. It goes to the political views of political parties, and under privacy law, sensitive information is normally entitled to greater protection.

Right now we have no protection federally, except what political parties choose to put in their own privacy policies without any legal requirements, so I think it would be a very good thing for political parties to be subject to privacy laws.

For instance, with the CPPA, it could be possible to add a provision that would extend the CPPA to political parties, recognizing the sensitive nature of that information.

● (1710)

Mr. Brian Masse: That's great.

Mr. Kardash, you have whatever time is left.

Mr. Adam Kardash: I'll be brief.

My view—and we've thought about this quite carefully—is that there is no public policy rationale for the political parties' processing of personal information not to be subject to a privacy legislative regime. The only question that I think is open is what the appropriate instrument would be and whether that would that go into the CPPA. I think there's some validity to the proposition that it might be a separate instrument. My personal view is that it was something that was missing in Bill C-27. It could have been in there.

Right now, if you compare the privacy protections that are set out in Bill C-27 under the CPPA to the current protections afforded to individuals in respect to the processing of personal information by political parties, you see that they're not even in the same universe. You would just have to post a privacy statement. There's no security breach notification requirement. There are no access rights and no consent rules. It goes on and on. There are no rights of express redress. There's no independent ombudsman who would oversee and take complaints, investigate, etc.

I think this is something that is incredibly important and I'm very thankful to you, Mr. Masse, for bringing that up.

The Chair: Thank you, Mr. Masse.

I'll now turn the floor over to Mr. Perkins.

Mr. Brian Masse: Thank you.

Thank you, Mr. Chair.

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

This has been very interesting testimony.

Mr. Therrien, I'd like to follow up on MP Vis's initial questions on the issue of minors. The only place in the bill where “minor” is mentioned is in the “Interpretation” section at the beginning.

It doesn't define a minor, and I think a lot of us are in agreement that this bill should define the age of a minor, but it also says in this act that “the personal information of minors is considered to be sensitive information”. For the life of me, when I look through this act, I don't see any definition of “sensitive information”.

Mr. Daniel Therrien: Indeed, the concept of sensitive information is currently undefined under the current law and would be under the proposed law. That normally leads to what is called the “contextual application” of what is sensitive: It's what kind of information is at play. Is it financial? Does it concern children or health? That would be generally sensitive information under “Interpretation”, but there's no definition in the law itself.

Is it a flaw that there is no definition? At the end of the day, the definition will always be contextual. I think it is possible, though, to have a definition that would be non-exhaustive and refer to certain factors—financial, health, children, etc.—as factors that would be defined is normally sensitive information, leaving an out clause, a residual clause, for what is not defined. I think that would be an improvement.

Mr. Rick Perkins: As a person who has spent most of his career as a marketer, I love data, and I would go to the edge as much as possible with what I was aware of and what I could do with that data, but I'll tell you that this bill and those aspects would make me nervous. I just don't see, as a marketer, any guidelines that help me to figure that out, and I suspect that most marketers would push the envelope, as they do, and might end up in trouble for their company. I appreciate that there should be more definition.

I'd like to go back to my earlier question.

Mr. Therrien, proposed subsection 15(5) outlines that “implied consent” is okay. Personally, I don't think implied consent is ever okay. Do you see it as an issue in this bill that implied consent is allowed?

Mr. Daniel Therrien: Implied consent is certainly open to broad interpretation and is sometimes abused, but it is a concept that exists under most, if not all, privacy laws that I know of. It is a recognition of the fact that in today's technological environment, you cannot realistically ask people to consent explicitly to every use of information that will be made.

On the issue of what amendments to make to the consent regime, I would maintain my recommendation to align the language of proposed section 15—not subsection (5), but another provision—to the current section 6.1 of PIPEDA.

● (1715)

Mr. Rick Perkins: The problem with the proposed subsection 15(5), which also ties to proposed subsection15(6), which also ties to proposed subsection 18(1) and proposed subsection 18(2), is that the implied consent is allowed on a wide variety of things, including “any other prescribed activity”— whatever that is. It leaves it wide open.

Earlier in the bill, in the consent section, it says that if express consent is required and if there is a new provision or a new use of that person's data, the express consent needs to be given again.

It seems to me that this is contradictory, in saying, “Well, I can apply it anyway. I don't have to pay attention to the earlier part of the bill that says I have to get express consent for a new purpose, except when I look at proposed subsections 15(5), 15(6), 18(1) and 18(2).”

Mr. Daniel Therrien: My answer to that would be pay attention to the provisions that define purposes for which businesses can use information. Right now, I think it is fairly open-ended. There are not many, if any, limitations, except under proposed section 12.

If the provisions that define original purposes or new purposes were to say that only specific and explicit purposes are lawful, then I think that would be a step forward.

Mr. Rick Perkins: I have one last question.

Who should own a person's data, me or the organization?

Mr. Daniel Therrien: Certainly that's the six-million-dollar question currently. It goes to the history of technology and legislation, the fact that many decades ago, the consent model was seen to be the best model—which assumes a lot of control.

I think we've not left that world. There is still value in people controlling their information to the extent possible, but realistically, we know that we're no longer in that world. It is simply not realistic to think that citizens can provide consent in each and every case when information is used. We need to accommodate a world where consent is not required, but, I maintain, within a model that protects privacy as a fundamental right, including the four provisions that I mentioned earlier.

The Chair: Thank you, Mr. Therrien.

Mr. Sorbara is next.

Mr. Francesco Sorbara (Vaughan—Woodbridge, Lib.): Thank you, and good afternoon, gentlemen.

I apologize for missing your earlier testimony for a pre-existing appointment.

Adam, you made a comment earlier about the bar on personal data—I may have forgotten the words exactly—in terms of how we identify personal data as being owned by the individual or not owned by the individual, or identifying it. Can you elaborate on that point?

If it wasn't you, I apologize, but there was a reference to that.

Mr. Adam Kardash: I think it might have been a reference about the current bar of when data is identifiable or no longer identifiable.

Mr. Francesco Sorbara: Yes.

Mr. Adam Kardash: First of all, the concept of personal information, or more specifically identifiability, is well established in Canadian jurisprudence. If there is a serious risk of possibility of identifying an individual directly or indirectly or just contextually, it will be deemed to be identifiable. That is a very high bar, given the environment, especially the contextual part, as there is more dynamic data and more data, etc. That's what I was speaking to.

The injection of our proposed amendment was to align the current definition of “anonymize” in the CPPA to ensure that we're consistent with the jurisprudence and consistent and interoperable with the statutory regimes across the country.

Mr. Francesco Sorbara: As a non-lawyer, I wonder if the bar is too high, too low, or...?

Mr. Adam Kardash: Very simply, the bar set out in the current text of the CPPA is too high. It's practically unworkable. A simple surgical amendment, as recommended by CANON and others, would address it, and it would address it in a way that's totally consistent with other legislative regimes.

● (1720)

Mr. Francesco Sorbara: Bill C-27, in my humble view, is a groundbreaking piece of legislation. I'll use that term. I think it is groundbreaking in terms of the update it's providing to the act and to privacy.

Mr. Therrien, you're fully versed on privacy issues relating to Canadians. When I think of this bill and I think of my constituents back in the city of Vaughan in my riding of Vaughan—Woodbridge, I would tell them how their privacy is being protected and not being protected on a very granular basis. I would use layman's terms. What would you tell me to tell them in terms of your view of BillC-27?

Mr. Daniel Therrien: You may be referring to whether the law should be principles-based or rules-based, for instance—

Mr. Francesco Sorbara: If I could interject, as a finance person and someone with an extensive accounting and finance background, I know principles-based and rules-based matters, so yes, please....

Mr. Daniel Therrien: I think on the aspect of risk, it's a bit of both. Currently, PIPEDA is principles-based—there are some rules, but rules are few. CPPA would certainly keep principles but adopt many more rules. I think an effective system has both principles and rules that are at a sufficient level of generality that they can still be relevant even if the technology or the business context changes over time.

I think where I would disagree with my colleague Mr. Fraser is that PIPEDA lacked the rules that would ensure protection. I'm not suggesting a prescriptive statute, but I'm suggesting a statute that has both principles and actual rules stated at the right level of generality.

Mr. Francesco Sorbara: I have a final question.

When producing legislation or enacting legislation, we obviously want the legislation to be robust to handle evolving technologies—in this case, evolving situations. Where we are today is vastly different from where we were 10 years ago in privacy and in AI and just the technologies, I think. The legislation we have in front of us, in my view, has that robustness, but obviously you folks are much more expert on this front. How would you characterize the robustness in this legislation to handle the evolving environment we're in?

Mr. Kardash can begin. Then we can go across if we have time.

Mr. Adam Kardash: The legislation is drafted in a technologically neutral and sectorally agnostic way, so that will serve Canadians well, and organizations trying to comply with it, because it will allow for the evolution of practices over time to deal with that, so I think that's really helpful.

I also think that while it's often referred to as a consent-based regime, fundamentally it's an accountability-based regime. I can't speak for my other colleagues, but I think there's broad-based agreement that Canada has actually led the way internationally with this accountability model. It's been adopted otherwise, and now it's been strengthened.

You have the combination of the accountability model with some careful drafting, with some enhancements to privacy protections that I think will serve organizations and, in particular, Canadians well.

Mr. Francesco Sorbara: I'm not sure if we have time, Chair, but perhaps Mr. Fraser or Mr. Therrien would like to land on that.

Mr. David Fraser: I think it will ultimately prove to be a resilient piece of legislation. I don't see potholes or anything else like that, or pitfalls such that we're going to have to come back to revisit it in five or 10 years' time necessarily.

Mr. Francesco Sorbara: Thank you.

Thank you, Chair.

The Chair: Thank you, Mr. Sorbara.

We have five more minutes, so I'm willing to open the floor. I'll yield the floor to me first—

Voices: Oh, oh!

The Chair: —with consent.

Maybe you won't like the question I'm about to ask, but if we were to include political parties in the act, what would be the lowest-hanging fruit that could be included, and the most important one?

This is for Mr. Therrien and Mr. Kardash.

[*Translation*]

Mr. Daniel Therrien: I think you could include rules on disclosure by political parties and others on use. The worst possible case was that of Cambridge Analytica, a company that authored certain practices aimed at influencing voters. If political parties were subject to privacy laws and these practices continued to be used, at least penalties could be imposed on those who obtain this type of information. There's a whole range of consequences.

Rules on the protection of information—that is to say security mechanisms—could also be included. These issues are currently the subject of voluntary measures on the part of political parties. If the parties were subject to the laws, there would be legal consequences for not protecting the information properly.

● (1725)

[*English*]

The Chair: Mr. Kardash, would you comment?

Mr. Adam Kardash: I would say rights of redress to the Office of the Privacy Commissioner of Canada, security breach notification requirements, rights of access so that individuals have an understanding of the personal information that is in parties' custody and control. I would say—and I missed the beginning of the remarks from Mr. Therrien—that I think there's the wave of other fair information practices that are encapsulated within the statutory regime.

Again, I just don't think it can be overstated that this is something that's really missing, and from a broader discourse, we're all focusing.... The digital charter rightly focuses on trust, and in order to establish trust, we need all participants to be subject to the same rules, etc., and I think political parties should be subject to those rules as well.

The Chair: Thank you very much. This concludes my questions.

We still have four minutes. I recognize Mr. Lemire and then Mr. Perkins.

[*Translation*]

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

Mr. Therrien, in the context of Bill C-27 and, more specifically, in the context of artificial intelligence, I would like to hear your opinion on industry self-regulation standards. That is, I would say, the new approach that is being put forward, both in Europe and by Mr. Champagne as a temporary or transitional measure. Can we trust industry to regulate itself?

Mr. Daniel Therrien: Over the past 20 years, we have clearly seen that there are significant limits to self-regulation. That is why it is currently necessary to amend the legislation and to provide for penalties, among other things.

In terms of artificial intelligence, again, it's not emerging technology, but its application is now becoming much more important. I think it would be a mistake to try to regulate it too precisely, too quickly.

So I wouldn't just rely on self-regulation. I don't think Mr. Champagne does either, since he is talking about self-regulation on a temporary basis while waiting for the upcoming act and regulations. In my opinion, it takes this legal architecture of an act, regulations and codes of practice for companies to have the best possible protection. Self-regulation alone is not enough.

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

The Chair: Thank you.

Mr. Perkins, you have the floor briefly.

[*English*]

Mr. Rick Perkins: I had two, but I'll start with one.

Proposed section 35 says that an organization may disclose an individual’s personal information without their knowledge or consent if it is collected for statistical purposes or research.

It doesn't identify by whom, but it seems to me to be a fairly open-ended breach of consent being that it can be given to the government for statistical reasons or to a university for statistical reasons or research reasons without going back, and it's personal information.

Could you comment on that, Mr. Therrien and Mr. Fraser?

Mr. David Fraser: There are already provisions that are similar to that in PIPEDA and other statutes, but with more safeguards that would a require privacy impact assessment, a research ethics approval, or reporting to the Privacy Commissioner. There are also provisions in the Statistics Act that allow Statistics Canada to compel that sort of information.

I share your concern when it comes to something that's so open-ended. One of the things that's a hallmark of good privacy accountability is an analysis and a determination of the inherent privacy risks and the mitigation steps that we can take. One thing I would also notice is that so many of those provisions are discretionary. They don't require the organization to disclose it; they permit it to do so.

● (1730)

Mr. Rick Perkins: Okay.

Mr. Therrien...?

Mr. Daniel Therrien: I would extend your question to a discussion that occurred a few minutes ago. I think here we're into the use of data for social good. It's an example of the use of data for social good. As Mr. Fraser said, there are similar provisions in the current act. I think these are good provisions, provided that we really deal with the social good.

Proposed section 39 otherwise defines “socially beneficial purposes”. Some of my colleagues have remarked that socially beneficial purposes are limited to disclosure to public entities. They make the point that private sector entities should be able to benefit from this. It's not inconceivable, but we need to be careful to disclose information to business for socially beneficial purposes. There's—

Mr. Rick Perkins: But proposed section 35 doesn't say that.

Mr. Daniel Therrien: No. Proposed section 39 does. That's why I expanded your question to deal with social good and included proposed section 35, statistical purposes, and proposed section 39, socially beneficial purposes. I would say that legitimate interests are the true domain of corporations. I think that latitude given to companies can be defensible. Socially beneficial purposes are currently limited to public entities, with the possibility of prescribing, by regulations, other entities, which I assume means potentially—

Mr. Rick Perkins: But it doesn't say that in proposed section 35. In proposed section 35, it's open to anybody.

Mr. Daniel Therrien: Yes.

Mr. Rick Perkins: It's any organization. It doesn't restrict it to social good. It doesn't have any restrictions whatsoever. It just says that an organization, if they decide to, can breach your personal information, do it without consent, and provide it to other people for “statistical purposes” or “research purposes”. That's to anybody. It doesn't say to business. It doesn't say to universities. It doesn't say to the government. It's available to anybody, under this.

Mr. Daniel Therrien: This has been interpreted, so far, as essentially in the domain of public interest statistical purposes, as opposed to purely commercial.

Mr. Rick Perkins: But businesses do research. Biotech firms do research.

Mr. Daniel Therrien: I understand.

The Chair: Thank you very much.

[*Translation*]

That's all the time we have for this meeting.

I want to thank all the witnesses for taking the time to come and meet with us today. This has been a really interesting discussion.

I thank the support staff, the interpreters and the analysts.

The meeting is adjourned.