HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 047 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, February 16, 2017

Chair

Mr. Blaine Calkins

Standing Committee on Access to Information, Privacy and Ethics

Thursday, February 16, 2017

● (1530)

[*English*]

The Chair (Mr. Blaine Calkins (Red Deer—Lacombe, CPC)): Good afternoon, colleagues.

I'd like to get straight to business.

I will remind colleagues that the supplementary estimates were tabled in the House. There were no supplementary estimates that affected anything in the purview of this committee, so this committee will not have any supplementary estimates to review.

In this first hour of our second meeting on the study of PIPEDA, we are pleased to have, from the Office of the Privacy Commissioner of Canada, the Privacy Commissioner himself, Mr. Daniel Therrien. With him is Patricia Kosseim, senior general counsel and director general, legal services, policy, research and technology analysis branch.

Does that all fit on a business card? Actually, I shouldn't ask you questions like that.

We have Brent Homan here, as well. He is the director general of Personal Information Protection and Electronic Documents Act investigations. He's the top guy for PIPEDA.

Mr. Therrien, perhaps you could enlighten us with your opening remarks. Then we'll get in as many questions as we possibly can in the first hour.

We thank you once again for appearing before the committee.

[*Translation*]

Mr. Daniel Therrien (Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada): Thank you very much, Mr. Chair.

Members of the committee, thank you for inviting us here for your study of the Personal Information Protection and Electronic Documents Act, the PIPEDA.

As you know, PIPEDA is technology-neutral and based on principles of general application, two qualities that should remain as these are strengths that make this law a flexible tool.

However, the constant and accelerating pace of technological change since the turn of the 21st century, when PIPEDA came into force, is challenging the law's effectiveness and sustainability as an instrument for protecting the privacy of Canadians.

These technological changes bring important benefits to individuals. They greatly facilitate communications, they make available a wealth of information of all sorts, and they bring products and services from all areas of the world.

But these technologies also create important risks. Internet users want to share their views and search sensitive issues like health without fear that these activities will be tracked and shared with others with adverse interests. In fact, it is an essential aspect of the right to privacy that individuals have control over with whom one they share their personal information.

New technologies also hold the promise of important benefits for society. Future economic growth will come in large part from growth in the digital economy. For instance, Canada is well placed to become a world leader in artificial intelligence, which depends on the collection and use of massive amounts of data.

The 2016 OECD Ministerial Declaration on the Digital Economy, to which Canada is a signatory, commits, among other things, to an international effort to protect privacy, recognizing its importance for economic and social prosperity. Indeed, the protection of privacy is critical for building consumer trust and enabling a vibrant, robust and competitive digital economy.

Yet, the vast majority of Canadians are worried that they are losing control of their personal information, with 92% of Canadians expressing concern, and 57% being very concerned, about a loss of privacy in our most recent public opinion poll.

Without significant improvements to the ways in which their privacy is protected, Canadians will not have the trust required for the digital economy to flourish, they will not reap all the benefits made possible through innovation and, ultimately, their rights will not be adequately respected.

Consent has always been considered a foundational element of PIPEDA, but obtaining meaningful consent has become increasingly challenging in the age of big data, the Internet of Things, artificial intelligence and robotics.

When PIPEDA was adopted, the interactions with businesses were generally predictable, transparent and bidirectional. Consumers understood why the company that they were dealing with needed certain personal information. It is no longer entirely clear who is processing our data and for what purposes.

As such, the practicability of the current consent model has been called into question.

To be clear, I think there remains an important role for consent in protecting the right to privacy, where it can be meaningfully given with better information.

There may also be situations in which consent is maybe simply impracticable, and under appropriate conditions, it is worth exploring whether alternatives to consent can otherwise protect the privacy of Canadians. Some of these may require legislative amendments.

Through written submissions and in-person consultations with stakeholders across Canada, we've heard a broad range of suggestions.

For instance, individuals could be empowered to make decisions through simplified privacy notices. Organizations, on the other hand, could enhance their trustworthiness through the use of privacy by design, demonstrable accountability, or the adoption of industry codes of practice.

● (1535)

We heard that some wanted us to provide further guidance for organizations or promoting compliance through more proactive means such as audits. Others wanted us to have greater enforcement powers, a point to which I will return.

We also heard consistently that public education is essential and that more needs to be done.

We have therefore consulted a great many Canadians on the issue of consent. We are currently analyzing the proposed solutions, and many others in our general findings on the matter. We will be happy to share our consolidated findings with you once we have completed our work in mid-2017.

[*English*]

Another priority area for our office is reputation and privacy. Our ultimate goal here is to help create an environment in which individuals may use the Internet to explore their interests and develop as persons without fear that their digital trace will lead to unfair treatment.

As with the consent project, we started our work by issuing a discussion paper and inviting submissions. Many of the submissions received commented on the right to be forgotten, the concept arising out of the EU that individuals can request that certain links be removed from search results associated with their name. While acknowledging the potential harms that can come from a net that never forgets, some submissions raise significant concern about what a formally recognized right to be forgotten would mean for freedom of expression. Others question whether PIPEDA even applies to a number of aspects of online reputation or to search engines that are important players in that debate, and they call for other solutions instead. These ranged from greater use of targeted legislation to prevent specific harms, as we have seen in the cases of cyber-bullying and revenge porn; improved education on safe and appropriate use of the Internet, especially for vulnerable populations; and improved practices for websites and online services such as social networks. We would be pleased to inform the committee of our views once our policy position has been fully shaped later during the year.

Let me now turn to the question of enforcement powers. Enforcement is key to securing trust in the digital ecosystem. Our recent poll found that seven out of ten Canadians would be more likely to do business with companies if they were subject to financial penalties for misusing their information.

Currently my office cannot make orders or impose fines and it is, in many respects, weaker than some of our provincial and international counterparts. Industry worries that, should enforcement powers be granted to my office, organizations would be less willing to collaborate with us and negotiate toward solutions, yet my colleagues elsewhere have not had that experience. Perhaps it is time, then, to bring my office's powers in line with those of others around the world.

That being said, I also believe there is an important role for proactive compliance. Organizations are using data in innovative ways to derive value, and Canadians expect this activity to be regulated. A proactive approach to overseeing compliance at the front end before complaints happen would bring certainty to the market and further reassure Canadians that their concerns are being addressed.

Given time considerations, I will stop here, but let me conclude—can I continue?

● (1540)

The Chair: Please do. You're the commissioner, sir.

Mr. Daniel Therrien: I have some notes on adequacy. I assume there will be questions about adequacy. I can speak about that if you want.

The Chair: Please do. Please finish your presentation.

Mr. Daniel Therrien: All right.

Adequacy is another issue that I think the committee should bear in mind during its review: the adequacy of privacy laws in Europe. In Europe, the GDPR, the general data protection regulation, which has been adopted and will come into force in 2018, will require a review of adequacy decisions every four years, and Canada's adequacy status, which since 2001 has allowed data to flow freely from the EU to Canada, will have to be revisited.

A January 2017 communication from the European Commission notes that Canada's adequacy status is “partial”, in that it covers only PIPEDA, and that all future adequacy decisions will involve a comprehensive assessment of a country's privacy regime, including access to personal data by public authorities for law enforcement, national security, and other public interest purposes.

Given the far-reaching impacts of our country's adequacy status on trade, as well as the differences between GDPR and PIPEDA, it will be important to keep this consideration in mind as the committee moves forward with its study.

In conclusion, Professor Klaus Schwab, founder of the World Economic Forum, states that we stand on the brink of a fourth industrial revolution, characterized by a blurring of lines between the physical, digital, and biological spheres. This transformation, he argues, will be unlike anything humankind has experienced before.

PIPEDA was good legislation when it came into force in 2001, and it continues to provide a sound foundation upon which to build. However, in light of this new revolution, and more importantly, to meet the privacy expectations of Canadians, I believe that PIPEDA must be modernized.

Thank you very much. I look forward to your questions.

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

We'll now start with our seven-minute round.

Mr. Saini, go ahead, please.

Mr. Raj Saini (Kitchener Centre, Lib.): Good afternoon, Mr. Commissioner and everybody. It's always a pleasure to see you here. It seems as if we see you every fiscal quarter, so that's always very good.

We had some witnesses who came here on Tuesday. One of the important things that were recognized was the fact that Canada has a comparative advantage in North America, and indeed compared with other countries, because of our privacy laws, which are very commensurate with Europe's. Now with Europe launching a new level of regulation in May of 2018, there has been some discussion that Canada must change its privacy laws to be commensurate with those of the European Union.

Can you provide some commentary on what you think we should do or what specific aspects are necessary to not lose that comparative advantage, especially since now we're in the process of finalizing, or I guess we've passed, CETA?

● (1545)

Mr. Daniel Therrien: Yes. There is no absolute certainty in these matters, but I will give you my sense of what the considerations are.

The bottom line is that I think the committee should give serious consideration to reviewing any gaps or differences that may exist between Canadian privacy law and European law, because ultimately, under the European regulation, Canada's laws will be assessed—at the latest in 2022, four years after the coming into force of the GDPR—as to whether our laws are adequate, i.e., essentially equivalent to European laws.

Now, I say that there is no certainty in this matter because this standard of “essential equivalency” has not been defined very precisely by Europe. We know that equivalency does not mean “sameness”, so Canada's laws will not be expected to be a carbon copy of European laws, but still the standard appears to be quite high. It's one of essential equivalency. There may be some differences, but ultimately the laws should be essentially similar.

There are two areas in which potential differences between Canadian law and European law will have to be looked at. The first area is any differences between PIPEDA and the European regulation, the GDPR. The GDPR adds a few new rights to European law, one being the right to data erasure, which is the child, so to speak, of the “right to be forgotten”. That's one right that does not exist, per se, in Canadian law but exists in European law, and we should give consideration to whether we should bring our law closer to European law, if not to the same place. There is a right to data portability in European law that I urge you to look at.

For Canadian law, as it pertains to private organizations, this is a bit of the landscape. An important development in Europe over the past few years has been a decision of the European Court of Justice, essentially the supreme court of the European Union, which held, in a case called Schrems, that adequacy decisions in Europe should relate not only to privacy laws in other countries that relate to private organizations but also to public sector laws, including laws that govern law enforcement and national security.

What the European Court of Justice said in that case was that U.S. laws, under the previous safe harbour agreement, were not essentially equivalent to European laws for a number of reasons, including the fact that they did not contain criteria of reasonableness and proportionality. I would urge you to have a look at our laws governing the public sector as well for equivalency.

One of the reasons why, in the context of Bill C-51, I recommended that the relevance standard be elevated to proportionality and necessity was the fact that in a few years our laws will be assessed against European laws, and European authorities will give consideration to necessity and proportionality as important factors.

Mr. Raj Saini: I also want to touch on something else you raised, because there is an interesting point to be made here. I'm referring to the case of Google Spain. I'm sure you're aware of the case of Google Spain. What I found interesting in that case was that the search engine was told not to provide a link to the news article, but the news article was still deemed to be allowed to exist. It wasn't ubiquitous, but it could be searched.

You talk about the right to be forgotten. If we decide to make that a recommendation, how do you think we should structure the law to allow someone the right to be forgotten? What parameters do we go through? Do we go all the way and remove everything? Or are there some things that have to be there for the public interest or the public good? How do we balance that?

● (1550)

Mr. Daniel Therrien: At the OPC we ourselves have not reached a conclusion on this point. We have issued a discussion paper. We have sought comments by stakeholders, and we are in the process of determining what our position should be. As I mentioned in my opening remarks, some of the submissions we have received are very critical and signal that, in Canada, the constitutional protection of freedom of expression may be slightly different from that in Europe and may lead us to a different outcome from the one in Europe. I'm not saying this is right or wrong. I'm saying this is a credible argument that needs to be seriously considered.

Beyond constitutional law we also heard from stakeholders that the way in which PIPEDA is currently constructed may not be consistent with a right to be forgotten. Particularly when search engines conduct search activities, they may not be governed by PIPEDA, because PIPEDA is consent-based and search engines do not require consent before they put results on their website.

So both as a matter of constitutional law, freedom of expression, and as a matter of statute law there is a gap as to whether PIPEDA applies. Should we close the gap? That's where I say it's very uncertain. Europe will require essential equivalency. It doesn't mean sameness. Presumably when they assess our laws they will consider differences in constitutional protections, for instance, on freedom of expression. So I think we should look at this question of the right to be forgotten. It is certainly consistent with privacy notions generally that information should not sit on servers or continue to be retained by organizations beyond the period when it's necessary. So should we look for exactly the same thing? Probably not. We should aim to go towards a right to be forgotten, but I don't think we need to reach the same place.

The Chair: Thank you, Mr. Commissioner. We're well past the time.

Mr. Jeneroux, go ahead, please.

Mr. Matt Jeneroux (Edmonton Riverbend, CPC): Thank you, Mr. Chair.

Thank you, Commissioner, for returning, and Brent and Patricia as well.

I'm picking up on Mr. Saini's point. Do you have a timeline as to when you're going to have this policy position on the right to be forgotten finished?

Mr. Daniel Therrien: Our first train stop will be the consent paper in mid-2017. After that we will issue a position on reputation, including the right to be forgotten. In all likelihood that will be by the end of this calendar year.

Mr. Matt Jeneroux: Okay. I was hoping it could coincide with the work of our committee here too. You've indicated that one of your priorities, reputation in privacy, is a major factor with regard to keeping up with the European Union. I also understand that you've submitted the names of some stakeholders for us to speak with as well. The EU has done this, but can you point us in the direction of any other jurisdictions that may have gone down this path that we could explore as well, particularly for the right to be forgotten but also for the legislation in general?

Mr. Daniel Therrien: I don't know if Patricia will be able to add something. The only thing that comes to mind is a recent judgment by the Japanese supreme court, which addressed this issue without recognizing the right to be forgotten per se. If did outline a number of factors that companies should bear in mind with regard to similar requests. Is there anywhere else?

Ms. Patricia Kosseim (Senior General Counsel and Director General, Legal Services, Policy, Research and Technology Analysis Branch, Office of the Privacy Commissioner of Canada): No, there is not in the positive. But south of border there has been enormous refraction to the right to be forgotten for reasons related to their First Amendment right of freedom of speech. There's an example of a jurisdiction that's likely not going there.

Mr. Matt Jeneroux: I find it fascinating, because I imagine that on the other side of someone's right to be forgotten are those individuals who would say they don't want to forget something that perhaps somebody else would prefer to be forgotten. It's an interesting argument, so I'm hoping we can flesh out some of that. Again, if anything comes out of your policy discussions in the lead-up to it, I hope we would get it before the committee.

● (1555)

Mr. Daniel Therrien: Perhaps I could just add that, on the constitutional question from a Canadian perspective of freedom of expression and whether a right to be forgotten would contravene the charter, I think at the end of the day it's going to be a question of balance, balancing the right to privacy of individuals, which may include some form of a right to be forgotten, against the constitutionally protected freedom of expression. So I think we should be looking for a balance.

Mr. Matt Jeneroux: Okay, I appreciate those comments.

We had a Mr. Lawford from the Public Interest Advocacy Centre here at our first meeting. He brought up—it escapes me what he called it, but something along the lines of a child protection act. I'm curious to know if you have any thoughts or some guidance on where we go down the road with the child privacy protection.

Mr. Daniel Therrien: In the U.S., there is a statute—the acronym is COPPA, I believe—that prohibits the collection of information about children under 13. In Canada, we don't have that kind of legislation for a number of reasons. I think one is the fact that PIPEDA is framed in terms of general principles, one of them being consent. So consent is required for the collection, use, and disclosure of information. Consent must be meaningful and informed. For children under a certain age, certainly it cannot be informed or meaningful, so we don't have a definite age limit and an outright prohibition, but we get a similar outcome in a different way.

Certainly as well, I believe that because the age of majority in Canada is a matter for provincial legislators to legislate on, the federal PIPEDA has not sought to define an age of majority in the past. Now does that mean that it could not be done in concert with provinces to have an absolute prohibition? It could. This is something that could be done. But I think we get that, or something pretty close, with the legislation we have.

Mr. Matt Jeneroux: So you're comfortable with the current legislation. I guess that's why you didn't bring it up in your submissions or your statements today: you're comfortable that it's handled.

Mr. Daniel Therrien: There is certainly a level of protection for children. It doesn't reach the level of an absolute prohibition, but there is a level of protection. So, yes, I'm comfortable that it exists.

Mr. Matt Jeneroux: Okay.

I think I have a minute left.

I want to give you a little bit of time to flush out some of your answers on enforcement powers in particular, because I imagine—and you've been through this process before—we're going to have a number of private individuals, companies, and representatives come through here arguing the other side of it. You obviously are of the position that having enforcement powers is the right thing to do; however, I imagine some of them might spend time on the opposite. So if you have anything else you want to add on that front, please go ahead.

Mr. Daniel Therrien: Thank you. The first reason I think you should consider giving us stronger enforcement powers is that our reading of the expectations and the will of Canadians is that we should have these powers. We have consulted Canadians regularly over the years, and the percentage of Canadians who say, for instance, that they would be more likely to do business with an organization if the organization were subject to order-making or fines is higher than 70%. In the context of our consent consultations, we have conducted a number of focus groups, and when we ask them whether they think it would be a good idea for companies to be subject to orders and fines, they overwhelmingly say it would be a good idea, so I think Canadians expect it.

In terms of the importance of privacy that would come from that kind of a regime, we were told by companies during our consent consultations that, if the OPC had these powers, the current collaborative status that we have with companies might change. As I said in my remarks, that's not been the experience of other jurisdictions.

The experience of other jurisdictions is that having fines and orders that come with privacy violations changes the risk calculus for executives of companies. If an executive in a company has a choice between investing in consumer protection or environmental protection where there are fines that will potentially be imposed if there is a violation and investing in privacy where there is not, we were told quite point-blank that they will put their money where there is a financial risk.

So a not insignificant consequence of giving the OPC order-making and fine-imposing power is that it will change the risk calculus for businesses such that they will invest more in privacy protection, which I think is a good thing. Just the fact that these powers exist will change the risk calculus, whether or not we find them to be in violation of the act.

● (1600)

The Chair: Thank you very much.

Mr. Cullen, go ahead, please, for seven minutes.

Mr. Nathan Cullen (Skeena—Bulkley Valley, NDP): Thank you, Chair.

Welcome, Commissioner. I'm quite new to this topic, so forgive me if I trip over anything since I am profoundly ill-informed regarding what we're talking about. I do find it incredibly fascinating.

Can you give us a range regarding what the order-making and fining powers are like for our trading partners in Europe and the United States? What range of fines are we talking about? What is typical, and what would industry in Europe have grown accustomed to?

Mr. Daniel Therrien: In Europe, under the new regulation that will come into force in 2018, I believe the maximum will be 4% of the global revenue of a company.

Mr. Nathan Cullen: That's not insignificant.

Mr. Daniel Therrien: It is extremely significant.

Mr. Nathan Cullen: And is there any gradation at all between large firms and small and medium enterprises?

Mr. Daniel Therrien: By function of the revenue of the company, the maximum, 4% of global revenue, means a small company will pay a smaller amount.

Mr. Nathan Cullen: I understand, but we also know there's a grading scale of difference in the security capacity of a large multinational firm versus that of a mom-and-pop operation that has a small online retail business on the side.

Mr. Daniel Therrien: Here, I think we would take the difference in size into consideration in terms of our expectations of the kind of security a company would require.

Mr. Nathan Cullen: Okay, so there's some flexibility.

Mr. Daniel Therrien: Yes. In the U.S., I don't know the maximum—perhaps one of my colleagues can say—but there are fines in the millions of dollars.

Mr. Nathan Cullen: Sure. So your basic argument to Canadian industry is that, as we're in the midst of this new economic revolution, we are not realizing its full potential if Canadians don't feel trust when they go online to shop and participate, and that trust would be enhanced if they knew you had the powers to find bad actors. Is that essentially the argument?

Mr. Daniel Therrien: Yes.

Mr. Nathan Cullen: So it's in their own best interests.

Mr. Daniel Therrien: Yes.

Mr. Nathan Cullen: I'll put that to them when they show up at committee.

I'm concerned about what happens with personal information as we cross the border to the U.S. We saw the recent executive order from President Trump in late January excluding non-U.S. residents from protections under the U.S. privacy act. The information that is made available through things like NEXUS or the FAST pass that trucking operators use is extensive.

You have calmed fears that were raised several years ago. This personal information is extensive. This is biometric. Canadians give up a great deal of information when they cross the border. In the past, there have been protections under the U.S. Privacy Act, but under this executive order, no longer. Should this be concerning to Canadians as we see certain disruptions and certain people profiled, particularly Muslim Canadians?

Mr. Daniel Therrien: Yes, it should be a concern, although we are looking at this issue and we haven't concluded yet what the net impact of this new executive order will be.

● (1605)

Mr. Nathan Cullen: We can understand the concern, though, because the order says

> to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information.

That's disturbing and quite significant, considering the amount of traffic that goes across the border, including businesses seeking to do business. I spoke to a Vancouver company last week. It's an IT company. By some coincidence, half of their staff come from countries that Mr. Trump recently identified on his so-called Muslim ban list. Three-quarters of their clients are in the U.S. They do not trust their staff's ability to cross now. This is a growing Canadian company, a success story, and they can't send anyone over the border —whether because they could be stopped, demeaned, or other things that have happened so far, or because, on the information side of things, their employees no longer have confidence that there is any protection of their personal information once their NEXUS card is swiped.

Are there any concerns about that?

Mr. Daniel Therrien: Yes, we are concerned. What we're looking at is that the order eliminates or reduces protections under one specific legal instrument under U.S. law, the U.S. Privacy Act. There are a number of legal instruments in the U.S. that may give some protection: certain orders made by President Obama, for instance, or constitutional protections.

Mr. Nathan Cullen: Let's not name them. Trump might eliminate them if he hears about them.

Mr. Daniel Therrien: Possibly. We are concerned, but we're looking at it. It's a complex matter, and you need to look at all of the legal instruments at play.

Mr. Nathan Cullen: I understand that it's complex. I'm not a lawyer, so I can only envy those who have to go through this. I think there is a lot of uncertainty.

Mr. Daniel Therrien: Absolutely.

Mr. Nathan Cullen: That's what I am picking up from Canadian industry and from Canadians broadly about personal information in general, as you've noted in your statistics, especially with this extra element, xenophobia, placed on top by the U.S. administration. The issuance of such an order would be.... It has to be accurate, of course, but it would be incredibly helpful to be expedient in order to alleviate some of that. Does the Canadian government need to respond by informing Canadians who are seeking to cross the border to work in the United States, if they happen to be, as we have found, people of Moroccan or Iranian heritage, or anything else that happens to bother the current administration?

Mr. Daniel Therrien: We have received a communication from an NGO, OpenMedia, raising these issues, and we are actively looking at this issue. You asked whether the government should do something. I hope the government is looking at the impact. It should be looking at the impact of that order and communicating to Canadians what it thinks the impact of that order is.

Mr. Nathan Cullen: There is nothing yet. We've seen NEXUS cards seized. We've seen young Canadian athletes shielded from the border.

This is so far out of my depth, but I have a quick question about the gathering of people's information. When someone uses a free service—does a Google search or has a Facebook account—there is some shield that's afforded. Can you explain your interpretation of the law with respect to this, in terms of companies gathering and selling that data to a third party for consumer information? Is that the way the law exists right now, and should it be modified?

Mr. Daniel Therrien: Are you talking about information that is publicly available through social media, for instance?

Mr. Nathan Cullen: It's not public.... Well, it's nominally publicly available, but it's somebody's searches, interests, and social media activity gathered up by those companies—shielded because the service is offered for free—and then packaged and sold to consumer companies. We all know that if we type “shoes” in Google, suddenly shoe ads start appearing all over the place. There is no protection of that particular data being sold further on, is there?

Mr. Daniel Therrien: I would distinguish between two legal notions. You're referring to information that is on the net and under public settings, say, on social media. PIPEDA has a very restricted definition of what is publicly available and would not, per se, authorize the use and disclosure of information except if it fit the very narrow definition of “publicly available”, and in your example, it would not. That's one thing. It may be, though, that in the consent terms for the collection of information there may be a term between the consumer and the organization that would authorize the organization to use the information, to sell it to advertisers—

● (1610)

Mr. Nathan Cullen: Perhaps we'll talk about those consent forms in my next round.

The Chair: Thank you very much.

Next will be Mr. Erskine-Smith for a five-minute round.

I was very liberal. Everybody has gone well over their seven minutes, and we're not going to get through the five-minute round as a result. I'm going to ask colleagues to be very concise with their questions.

Mr. Erskine-Smith.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Thanks very much.

I wanted to begin with the recommendations of your predecessor with respect to PIPEDA. I want to start with enforcement powers, which you touched on.

There was no clear recommendation in Ms. Stoddart's view. She said there should be greater enforcement powers and that we were actually lagging behind other jurisdictions. Then she recommended statutory damages, the power to make orders, the power to impose administrative monetary penalties, or some combination thereof. She noted that, in 2013, the U.K. Information Commissioner's Office levied a £250,000 fine against Sony for a breach that affected millions of PlayStation users.

In your view, should we be looking at statutory damages? Should we be looking at giving you order-making powers, or should we be looking at giving you administrative monetary fining powers? What would be most effective?

Mr. Daniel Therrien: I would say a combination of order making and the ability to impose a financial sanction.

The other day, someone mentioned that perhaps this should be subject to certain parameters. We would be in agreement with that.

Mr. Nathaniel Erskine-Smith: Ms. Stoddart also recommended mandatory breach notifications, and noted that most U.S. states have passed similar legislation.

You would, I assume—

Mr. Daniel Therrien: That's part of Bill S-4, which will come into force soon.

Mr. Nathaniel Erskine-Smith: Excellent.

With respect to accountability, Ms. Stoddart recommended amending schedule 1 to require that organizations demonstrate, at your request, that they have practices in place for privacy compliance. She also recommended putting in place enforceable agreements under PIPEDA. Would you agree with that analysis?

Mr. Daniel Therrien: Yes, that would be an important, proactive action that we could take without waiting for complaints, absolutely.

Mr. Nathaniel Erskine-Smith: With respect to increasing transparency, Ms. Stoddart recommended public reporting requirements. This is with respect to an exception under PIPEDA for lawful authority. Law enforcement agencies are obtaining information from commercial entities. We currently have no public knowledge of how many times that has occurred.

Would you agree with Ms. Stoddart that there should be public reporting requirements to shed light on the exception under PIPEDA that allows law enforcement agencies and institutions to obtain personal information without consent or a warrant?

Mr. Daniel Therrien: Yes. We've made progress on that. Guidelines were issued by the Department of Industry some years ago. These are partially implemented. A legal requirement would improve things.

Mr. Nathaniel Erskine-Smith: You mentioned that you are working on a draft paper related to consent for mid-2017. You mentioned meaningful consent in your opening remarks. You also mentioned alternatives to consent.

There is no firm view from the OPC at the moment as to how we might update PIPEDA's consent model. I assume we'll get that in the report sometime mid-2017.

Mr. Daniel Therrien: I can give you the considerations we have in mind at this point, if that would help.

Mr. Nathaniel Erskine-Smith: Sure, that would be great.

In terms of alternatives to consent, one option that I noted from the previous commissioner was simplified privacy notices that draw attention to where practices differ from the norm and highlight information that would be most relevant to consumers. Perhaps you've reiterated that as well.

With respect to consumer protection law, sometimes there are provisions between consumers and companies that companies and consumers cannot contract out of because they're in the public interest of consumers.

If there are additional considerations, perhaps you could lay them out for us.

Mr. Daniel Therrien: There are a number of improvements that can be made without new legislation. Privacy notices are among them. I think it's a question of the will of industry to give better information to consumers before they collect their information. I don't think legislation is required to do that.

Public education and guidance on our part are also part of the solution. Those do not require legislation.

I'll tell you what we're grappling with, and I would suggest that you ask about the following things.

The reason the consent model is under challenge at this point is that when PIPEDA was adopted, the relationship between companies and consumers was essentially bilateral. There was a service provider, or somebody who was selling a product, and the consumer knew pretty well why their information was being requested. Now, the relationship is much more complex, particularly when the company is engaged in big data or artificial intelligence. The problem, from a legal perspective, is that the purpose for which the information is being sought and will be used may be extremely difficult to define upfront when the information is collected.

● (1615)

Mr. Nathaniel Erskine-Smith: So it's hard to clarify consistent use under PIPEDA then.

Mr. Daniel Therrien: Yes, because the purpose is difficult to define. Consent obtained from the consumer is not really meaningful, because the consumer does not know for which purpose the information will be used.

Mr. Nathaniel Erskine-Smith: But isn't it under the current law —and correct me if I'm wrong—that the individual consents to a particular purpose, and if there is an additional purpose, they have to go back and get consent from the consumer all over again?

Mr. Daniel Therrien: Yes, that is the current law.

We heard from companies during our consultations that the requirement to seek consent afresh once a specific purpose has been defined may be, in the view of some, too onerous or impractical.

But yes, as the law currently stands, the company would have to seek consent once the purpose had been defined. They're saying that it may not be practical. If so, we need a solution.

Mr. Nathaniel Erskine-Smith: Okay.

The Chair: Colleagues, based on the time on the clock and the fact that we have to transition from our first set of witnesses to our second set of witnesses—we have about 12 minutes—I'm seeking your counsel.

We have four questions, which would give us three minutes each, or I can just do two five-minute rounds. How would you like to proceed?

Mr. Matt Jeneroux: How about 12 one-minute rounds?

The Chair: Okay, I appreciate the decisiveness.

Mr. Kelly, go ahead for five minutes.

Mr. Pat Kelly (Calgary Rocky Ridge, CPC): Thank you.

I'd like to ask you to comment on consent and how this works in practice, in terms of the differences, and maybe issues that you....

Actually, let me ask this first. If I understood you correctly, you are in the process of preparing a paper on consent.

Mr. Daniel Therrien: We have issued a discussion paper seeking views, but without taking positions. We are going to take a position by mid-2017.

Mr. Pat Kelly: By the summer, you will have a position on consent. Okay.

For the record, could you briefly give us your own explanation, as simply as possible, of the distinctions between implied, informed, and express consent?

Mr. Daniel Therrien: Implied consent arises from the context of the situation, whereas express consent is sought specifically for a purpose for which the information is collected. That would be my simple explanation.

Mr. Pat Kelly: Is informed consent something in between?

Mr. Daniel Therrien: Informed consent means that the individual giving consent knows the purpose for which the information will be used and disclosed.

Mr. Pat Kelly: Do you currently have different models or different measurements by which you determine the appropriateness of the level of consent?

Mr. Daniel Therrien: The law is drafted generically, and I'll turn to my colleague in a second.

One problem is that organizations, companies, sometimes use extremely broad and generic language, such as saying that they will use and disclose your information “to improve customer experience”, and they seek consent on that basis. To me, that's not meaningful consent. The person cannot understand what will happen to their information if they are asked to consent to a better customer experience.

● (1620)

Ms. Patricia Kosseim: Thank you for the question.

Just to clarify whether it's explicit or implied consent, both need to be informed. In terms of PIPEDA, the validity of consent depends on it being of an informed nature.

In terms of distinguishing what form of consent is appropriate in different circumstances, whether it should be explicit or implied, in our guidance over the years, we have said that it will depend on the sensitivity of the information and the reasonable expectations of the individual. These factors will help inform whether the consent should be made explicit or whether implied consent would be acceptable in appropriate circumstances.

These factors were recently confirmed in a Supreme Court decision called Royal Bank of Canada versus Trang. In there, they confirmed those general conditions and set out a very helpful analytical framework for distinguishing situations in which explicit or implied consent would be appropriate in the circumstances.

Mr. Pat Kelly: Okay. How will the concept of consent affect a potential future law or legislation that defines a right to be forgotten?

Mr. Daniel Therrien: I think the two are distinct. Consent has to do with the conditions under which information is collected, used, and disclosed, and the right to be forgotten in our law has more to do with the retention period, how long a company can retain the information given the purposes for which it obtained it.

Mr. Pat Kelly: That would, in many commercial transactions, be part of what you consent to. I consent to the retention of information I give you for a specific period of time or I don't consent to that. Could the idea of being forgotten really be addressed that way? If a service provider has no right to retain information for longer than the period to which you've consented—

Mr. Daniel Therrien: It would help to prescribe a period of time for retention, for sure.

Mr. Pat Kelly: All right. In the interest of keeping moving, I'll finish with that.

The Chair: Thank you very much.

Mr. Bratina.

Mr. Bob Bratina (Hamilton East—Stoney Creek, Lib.): On that point, in *Mission: Impossible*, you agreed to this mission and the tape would be destroyed in five seconds, so why can't technology have sunset built into it, such that unless you're given a request.... I am just “blue-skying” on the subject. Could you conceive of a technological protocol that would allow for automatic destruction without consent of continuation?

Mr. Daniel Therrien: Yes, although it would all start with either a legal rule or a legal agreement as to what the period was. Once that was set then, yes, technology could make it happen.

Mr. Bob Bratina: I'm sure these conversations are taking place in many parts of the world. We have the Law of the Sea, and we have the International Civil Aviation Organization regulating air traffic. Should we not be having an international conference on these topics, or have you just come back from one?

Mr. Daniel Therrien: Two years or so ago, the United Nations appointed a special rapporteur on the right to privacy, and that person has a mandate to try to develop an instrument of international application, but this is not going to happen tomorrow. It's desirable, but this is not imminent for sure.

As for the right to be forgotten, I must say that if you ask whether there should be an international rule on something like the right to be forgotten, the right to be forgotten deals, as I said earlier, with the balance between important constitutionally protected rights, such as freedom of expression and the right to privacy. One aspect of privacy is that it depends on certain international principles, but its application depends a little bit on the culture of the place. All countries do not have the same way of looking at privacy, and certainly they do not have the same constitutional protections governing it. So, yes, we should move towards or we should seriously consider something like the right to be forgotten, but we should also look at our constitutional framework and values to determine how far to go.

● (1625)

Mr. Bob Bratina: Is there any real point in the long run, given that if you look at the case with banking, where you can hide your money in the Cayman Islands or someplace else, there could be offshore havens for data so that people would just hide the data somewhere else and draw it out when they would need it? Do you not see that as part of the problem with this whole question? That's sort of a spinoff of what you just said.

Mr. Daniel Therrien: Although an international instrument is not for tomorrow—I'll be more optimistic now—there are certainly discussions among countries on how to make privacy laws more congruent—not completely consistent but more congruent. Offices like mine co-operate for the enforcement of these privacy laws, to ensure that they result in similar outcomes. So we may not reach an international set of rules soon, but I see movement towards more consistency.

Mr. Bob Bratina: Thank you.

Thanks, Chair.

The Chair: We don't have enough time left for another five-minute round, so, colleagues, I don't know how you want me to deal with this. I think I'll just take up the last minutes, if that's okay.

Voices: Oh, oh!

The Chair: Mr. Therrien, I have a quick question for you. I was talking to the analyst here and something came across my mind, and it came out of the last meeting as well.

When electronic health records were brought up by a previous witness, we found, through a bit of investigation, that if the electronic health records or the data or the doctor's records—a person's medical records—were in a doctor's private practice, those would fall under provincial or federal private sector privacy legislation. Yet if that same medical record were in a hospital, it would fall under provincial or federal government privacy legislation, depending on where that document actually was.

If I give my accountant my information for tax purposes, the relationship with my accountant, I am assuming, falls under private sector privacy legislation. Yet my accountant is going to file my taxes on my behalf to the government, which then makes that information under the public sector privacy information.

So, with all of this overlap and confusion between private sector and public sector and information exchanging hands in this way, does it make sense that we have two sets of laws, one for the private sector and one for the public sector?

Mr. Daniel Therrien: The short answer is yes.

The Chair: That's all we have time for.

Some hon. members: Oh, oh!

The Chair: If you care to elaborate on that, that would be very helpful.

Colleagues, I appreciate your humouring me through this.

We thank you very much, Mr. Therrien, for coming once again. I'm sure it would be helpful, actually, at some point in time during the end of our study, once we've heard from more witnesses on this, to have you return to clear up some of the questions and concerns we'll have, so don't be surprised if you get an invitation.

We'll suspend for a few minutes, colleagues, to get ready for our next witnesses.

● (1625)

(Pause)

● (1630)

The Chair: We're resuming now. In order to keep to the agenda this time, I'm going to be much more strict on the seven-minute and five-minute rounds of questioning. That's the only way we can get through our one-hour time sessions. I am going to get straight to it.

We have, from the B.C. Freedom of Information and Privacy Association, via videoconference, someone who is no stranger to this committee, Mr. Vincent Gogolek.

We appreciate you joining us again today, sir.

We also have Ms. Valerie Steeves, who is appearing as an individual. She is a full professor in the department of criminology at the University of Ottawa.

Ms. Steeves, you have up to 10 minutes, so go ahead, please.

Dr. Valerie Steeves (Full Professor, Department of Criminology, University of Ottawa, As an Individual): Thank you very much.

First, I'd really like to thank the committee for undertaking this study. I think it's incredibly important and very timely, given the changes we've seen since PIPEDA was first passed.

When I think back over that period of time, I always find myself thinking about three things. PIPEDA, as you know, was enacted to create trust in the information marketplace. Second, when PIPEDA was being passed, it was quite clear that the intention was to create consent as a floor and not a ceiling. Last, data protection and the provisions that are included in PIPEDA were part of a larger strategy that was designed to protect privacy as a human right. At the time, PIPEDA was seen as a necessary part of this protection, but it was not sufficient in and of itself.

In the last 20 years or so, I've spent a lot of time doing research on children's attitudes and experiences with privacy and equality in network spaces. I think that research raises real concerns about the first of those points, the success of PIPEDA to create trust in the information marketplace.

You could argue that part of it is a lack of education. I was in the field talking to 13- to 16-year-olds in October and November. We asked them about fair information practices, and none of them was able to identify a single one of them. In fact, almost none of them could remember the point at which they consented to the collection of their information when they signed up or posted material on Snapchat or Instagram.

Certainly when you talk to young people about the regulatory regime, they talk about privacy policies, and they don't talk about them in a very flattering way. From their point of view, these have been purposely written to obfuscate and confuse them, so they won't know what's happening, and so they will feel powerless.

They repeatedly—and increasingly, actually, over the years—have told us that the commercial surveillance they experience on these platforms is creepy; and “creepy” is a really important word because typically it means that someone's privacy has been invaded. It's a marker. But at the same time, since their school lives, their home lives, their work lives, and their play lives are so interpolated with technology, they really feel they don't have any choice about it whatsoever.

I think a good starting point for your study is the recognition that even though so many Canadian young people and Canadian adults have flocked to these platforms, that doesn't mean they're comfortable with the current regulatory framework.

In 2015 we surveyed 5,500 kids between the ages of 10 and 17 across the country. We asked them, “Who should be able to see what you post online?” and 83% of them said that the corporations that own the platforms where they're posting the information should not have access to it. So if I put something up on Facebook, Facebook shouldn't be looking. And 95% said that marketers should not be able to see what they post. Whether they've posted in a public place or a private place, they felt it was private to them.

Typically when kids are talking about privacy, they're not talking about non-disclosure, they're talking about audience control, and marketers were not an audience they wanted or expected. Some 96% said that companies that sell them smart phones and other devices or apps that use GPS should not be able to use it to locate them in the real world; and 99% said that marketers should never be able to use GPS to figure out where they were in the real world.

I think this brief snapshot really strongly suggests that there is a disconnect between the regulatory model and the lived experiences of the people who play, shop, go to school, and hang out on these platforms.

I think that disconnect is really related to a bit of the fiction that's embedded in PIPEDA. PIPEDA assumes that, when someone posts a photo on Instagram or is keeping a streak going at midnight on Snapchat, they knowingly and consciously are undertaking a commercial transaction, that they are trading their personal information for access to the platform.

But from the point of view of the people who live on these platforms, it's not a commercial transaction. If I'm on Snapchat, I'm chatting with my friends, I'm doing my homework, I'm signing a petition, I'm exercising my free speech, or I'm exercising my freedom of association. I don't think that's an outrageous perspective. Certainly that's the same relationship we have with our land lines. Although I spend $70 a month so Bell can put a phone line in my house and I can talk to people, I certainly don't expect Bell to listen to my phone calls.

I had a painter in the other day. I don't expect Bell to interrupt my conversation with my painter and tell me, “Home Depot has a sale on paint right now”, and sell to me in that environment. And I certainly don't expect Bell to take all that information and run it through an algorithm to figure out if I'm a criminal or not.

If we go back and look at that time period, part of reconnecting to that earlier hope for PIPEDA, I think, calls upon us to place privacy or data protection in a much broader context.

● (1635)

Go back to the Finestone report of 1997, in which privacy was seen as a social value, a democratic value, and a human right. I think that broader perspective provides this committee with two advantages.

The first one is that it's exactly the kind of thinking that you're going to need to use if you intend to harmonize our privacy protection regime with the European general data protection regulation that comes into force and effect in 2018. I think it's arguable that Europe has done a much better job than North America has in navigating through the challenges we've seen in network spaces over the last 15 years or so, precisely because of a strong commitment to human rights and a strong jurisprudence working on that commitment.

I also think that this broader perspective, placing data protection as is necessary but insufficient on its own piece of protecting privacy as a human right, will help us navigate the consent debate more effectively. As I said, when PIPEDA was passed, it was very clearly articulated that consent was intended to be a floor and not a ceiling, and it sure felt like a leaky ceiling after about six months had gone by.

Particularly given the commissioner's comments on big data, certainly there's pressure to weaken consent provisions and there's pressure to make more information publicly available precisely so corporations can sidestep the provisions that we now have. There's more pressure to de-identify and to accept de-identified information as non-personalized information for the purposes of the legislation.

It's always for the promise of big data: if we can just keep all the information, we'll be able to learn new things, because artificial intelligence will identify patterns that are hidden to us, so that we can predict behaviour, we can be more efficient, and we can be more effective. I think privacy is the best way to crack that open and to begin to examine the ethical concerns that flow from this type of information use. Big data is not predictive. This comes back to my human rights concern. Big data is never predictive; it can look only to the past. It assumes that I will do in the future what I did in the past, but even worse than that, it assumes that I will do what people like me have done in the past.

There's a deep concern around these kinds of information infrastructures, which is that we will unintentionally and unconsciously recreate biases in our information systems. We'll either program them in through false proxies, or they'll be learned by the algorithms themselves. We can look at the example in England where they identified young criminals. The youngest potential criminal they identified was three years of age, and he was identified because he was racialized, he was impoverished, and he lived in a particular area. There are discriminatory outcomes that are hidden within this information management system.

Even if we take the position that the algorithm will be able to learn, I think all you have to do is look at what happened with Microsoft's Tay to realize that an open season on information will lead to unintended consequences that will harm the most marginalized in our society.

At a practical level, I have five suggestions.

I think we need to strengthen the reasonable purposes clause. I was lucky enough to participate in the commissioner's meeting on consent, and it was quite interesting. We had quite a debate, because the representatives of the businesses I was sitting with kept saying that businesses have a right to collect information, while I kept saying, “No, businesses don't have a right.” People have rights. Businesses have needs and desires. I found it quite interesting that they kept pointing to the purpose clause. I think there's an opportunity to enrich our commitment to human rights within PIPEDA by opening up and reaffirming the need to protect individual rights against business uses, rather than business “rights”.

Second, I imagine that you're seriously considering adding a right to delink information if there's no public value. It's the right to be forgotten clause. From young people's point of view, certainly, this is absolutely crucial. When you sit down and talk to young people about the risks they're worried about online, that's it. They say, “Oh, something I did when I was 16 is going to sink me, and I will never be able to get over it.” I think that's a particularly important area to examine.

Also, young people certainly ask for regulators to mandate more technical controls so they can more easily control their audiences and take down content. I'm personally quite concerned that community standards are being created by corporations and that our elected representatives are not active in that space of setting standards for the kinds of discourse that are appropriate in Canadian context.

● (1640)

Fourth, I'd strongly urge you to consider mandating some form of algorithmic transparency. So many of these practices are hidden, and it's only getting worse, and so I think corporations should be required to be fully transparent with their information practices, particularly because of this concern about discriminatory outcomes.

Last, I'd ask you to consider holding corporations to account for those discriminatory outcomes if they're going to get the benefit of access to this information. It's like pollution; somebody is going to pay for the dirty water. Since we're building this system right from the get-go, we should be considering who that burden should fall on, and I would argue that it should fall on the people who profit from it.

Thank you very much.

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

We'll now hear from Mr. Gogolek for up to 10 minutes.

Go ahead, please, sir.

Mr. Vincent Gogolek (Executive Director, B.C. Freedom of Information and Privacy Association): My apologies first of all, but I'm strictly limited to your 2:30 deadline because we're having a bit of a problem out here in British Columbia with a privacy breach, strangely enough, one that affects both the public and the private sectors. So, I will have to go at 2:30.

I will also try to keep my comments as brief as possible to allow the maximum time for questions. I will limit myself to the four points raised by the commissioner in his letter of December 2 to the chair, as well as two extra points.

We've also had two detailed submissions that we've put in to the commissioner's process, which I believe are available, and I'd be pleased to provide them to you.

Consent for the collection, use, or disclosure of our personal information is the underpinning of PIPEDA. Attempts to move away from this or to tamper with it should be viewed with considerable suspicion. At the same time, it's important to note that, in many cases, consent is really illusory. The conditions being agreed to are often in the form of over-broad, lengthy terms of service and other contractual services. The choice offered to consumers is often to accept all conditions or to not use the service. The result of this is that, in many cases, an organization feels free to do whatever it wants with the information it collects under the guise that the individual whose information it is has, in fact, consented to this.

For example, in our 2015 study on "The Connected Car"—which was generously supported by the contributions program of the Privacy Commissioner—we found that there were multiple agreements, policies, and contracts that come into play when somebody is attempting to purchase a vehicle. The purchaser is supposed to have read and understood all of these policies. At lot of times these are not available on the Canadian website of the manufacturer. They are available only on the U.S. website, and it's not entirely clear whether or not they apply. These policies and conditions tend to have very open-ended use and conditions that allow for "such other purposes as we see fit" or for research or for marketing. Some of these policies can, in fact, be somewhat contradictory. It's not entirely clear where these are coming from. As a result, we provide this general recommendation in our "The Connected Car" report:

> Rather than relying on the fiction of choice and consent, what is needed in this industry are clear, specific and relevant limits on collection, retention, use and disclosure of personal customer data. We need industry-specific data protection regulations for the Connected Car industry.

We also had a number of specific recommendations for the automotive industry regarding consent. I'd like to refer you to four suggestions that Professor Michael Geist of the University of Ottawa put forward as a useful basis for approaching the issue of consent generally: the opt-in consent should be the default model; rules on transparency must be improved; consumers must be able to exercise a choice other than to take it or leave it; and stronger enforcement powers and penalties are required.

In terms of reputation and privacy, with the rise of the online world, considerations that were once primarily the concern of the well-heeled and the well-known—things like damage to reputation—have become much more widespread and are, in fact, concerns of pretty much everybody who is involved online. What might once have been simply neighbourhood gossip can now become part of a global campaign of vilification. Ordinary people who do not have large financial resources or access to legal resources are put in the position of trying to defend themselves and their reputation in this new world. FIPA made a submission to the Privacy Commissioner's consultation on this issue, and I would refer you to that piece of work for a more detailed discussion of some of the issues involved.

● (1645)

We didn't make specific recommendations, but we did outline various considerations that should be taken into account when approaching this issue.

In terms of enforcement, as we've said before, with regard to the Access to Information Act and the Information Commissioner or the Privacy Act and the Privacy Commissioner, we're also of the view in terms of PIPEDA that the Privacy Commissioner should be brought up to the same level as his provincial counterparts who have order-making power. This system has operated for more than a decade in British Columbia, and there hasn't been any systemic problem with the commissioner having order-making power. It would also ensure that, in terms of protection of people's rights, they would be able to get a more immediate remedy under the federal regime, which is not the case currently, rather than somebody, say in British Columba, having a choice of complaining about conduct either provincially or federally.

In terms of adequacy, the order-making power would have, I think, a positive effect with regard to ensuring that PIPEDA continued to be looked upon as providing adequate privacy protections.

The two additional points that I would raise are these.

One is something that came up, I believe, during our discussions on the Privacy Act, and that is the coverage of federal political parties. It's our view that the federal political parties, which are currently not covered under any legislation protecting people's privacy and personal-information rights, should be dealt with under PIPEDA. Here in British Columbia, our substantially similar provincial act, the Personal Information Protection Act, covers the political parties in this province. Arguably it could cover provincially incorporated branches of federal parties. The commissioner has, in fact, successfully done at least two investigations and reports on the two largest parties here in British Columbia, and we continue to have parliamentary democracy here, so we don't see any impediment to federal political parties being brought under the PIPEDA regime.

Finally, I'd just like to support what Professor Steeves said in terms of algorithmic transparency. This is a very key point, and it's something that we raised previously with regard to the Privacy Act.

I look forward to your questions.

Thank you very much.

● (1650)

The Chair: Thanks a lot, Mr. Gogolek.

As I said, colleagues, I'm going to hold the line on the seven minutes this time; otherwise, we're not going to get through the full two rounds.

Mr. Bratina, please go ahead for seven minutes only.

Mr. Bob Bratina: Thank you.

Ms. Steeves, there seem to be two different behaviours to be addressed, on the consumer side and on the corporate side. On the consumer side, there's education, and on the corporate side, there's enforcement.

It's staggering, really, to hear you talk about young people's sense of what this is all about and the fact that they don't understand that they're really making a deal with the devil, if you will, by pushing that accept button. What serious measures could we take to address that?

Dr. Valerie Steeves: In the last review of PIPEDA, PIAC suggested that there be different levels, by age, of what could be collected from young people and no-go zones in which information would not even be collected from those under 13. Certainly developmentally speaking, you see that younger kids tend to be very mature and not put much out there. It tends to be the 13- to 15-year-olds who are most at risk.

I'm not sure if education is necessarily.... Certainly we do a lot of it. I do a lot of it myself, but I'm not sure if that's a fair response, because kids will say, "We're forced to use this technology at school. My mom makes me go on Facebook to check out my cousins so I can tell her what's going on, and at the same time I'm yelled at and told I shouldn't put any information out there." In the studies we've done with young people, it's quite clear that the platform is designed to create incentives to disclose.

I think we have to look at those incentives and really evaluate them, and this goes to the comment earlier about the need to really limit purposes. We create honey pots, especially with young people, and corporations collect everything because of these very broadly crafted clauses. If we were much more careful about the purposes of the collection, not just from a transparency point of view but by saying, "No, there are some things you just can't do", particularly with young people, I think that would go a long way.

● (1655)

Mr. Bob Bratina: You referred to the Finestone report, which was 20 years ago.

Dr. Valerie Steeves: Yes, I've been in this game too long.

Mr. Bob Bratina: Well, no....

I guess I'll have to dig it out and read it over and see how a 20-year-old report on this very subject resonates with today's reality.

Dr. Valerie Steeves: What's interesting about it is that it provides that broader context.

One of the things that I found when PIPEDA was passed was that prior to PIPEDA, the federal government exercised a great deal of leadership and put a lot of money behind public access points for technology. It supported non-commercial spaces like SchoolNet, which was a phenomenal site, and it created places where people could communicate and participate in public discourse without this deal with the devil, as you said. Once PIPEDA was passed, within two years, all of that was gone.

The federal government kind of exited from that type of leadership. I think it would be an interesting moment to go back and say, "Wow, what we meant to do was to create one piece of the patchwork that would deal with data protection within this broader quilt that looked at privacy as a human right."

The fact that we did not do it has actually put us behind the eight ball when it comes to a number of different issues, from national security to education. The stuff that's going on with educational software is terrifying.

Mr. Bob Bratina: Mr. Gogolek, we've had lots of great interventions from you, and I have to ask you this, because my time will run out soon.

For God's sake, if we don't do anything else, what should we be seriously looking at in terms of your priorities as to what needs to be done?

Mr. Vincent Gogolek: It's the question of consent and ensuring that it is in fact meaningful consent, informed consent.

We're very concerned about attempts to expand implied consent where you ought to have known that we would be using this. Somebody is saying "I agree" in order to use a service or a piece of equipment, and suddenly it's showing up in strange new places and having possibly very serious negative effects on them.

First of all, it's the notion that consent be real consent, as opposed to the idea that you checked the box so you opened yourself up to pretty much anything.

Mr. Bob Bratina: It's interesting. Sometimes I push the accept on a hand-held device that I can hardly see in my own hand, never mind find the button, but there's also a paragraph or two that goes along with that acceptance.

Mr. Vincent Gogolek: Yes, or sometimes there's more.

Mr. Bob Bratina: Sometimes there's more.

Thanks, Mr. Chair.

The Chair: Thank you, Mr. Bratina.

Now we'll move on to Mr. Jeneroux, please.

Mr. Matt Jeneroux: virtually. You're now in high definition, I think. It's a little clearer picture than we've seen of you before. You're looking good, sir.

Mr. Vincent Gogolek: Better than live.

Mr. Matt Jeneroux: Thank you, Mr. Chair.

Thank you both for being here.

Mr. Gogolek, it's good to have you back. I want to touch on the right to be forgotten. You didn't mention it too much in your speech, but I am curious as to whether you have an opinion on where we go.

I want to put the concept out there that Ms. Steeves mentioned about this being a real concern for young people, the millennials. They do something, X, at the age of 16, and that then impacts Y later on in their life.

There are certain times.... I guess I can understand the one side, but there's also the other side of that too. There are instances in which X would have a significant impact on Y, and we see this in politics. We saw it during the election campaign. I believe that a number of candidates in each party were impacted by something in their past or whatnot. When someone is running for public office, sometimes those things are important to know about.

I will open it up.

Mr. Gogolek, would you mind touching on the right to be forgotten? I'll ask Ms. Steeves for her response as well.

Mr. Vincent Gogolek: As an organization we don't have an official position on the right to be forgotten. We are not intervenors in either the Equustek-Google case or the Facebook case. In our submission to the Privacy Commissioner's consultation, we did set out some conditions that are important and some concerns that we have about how this is currently being done in Europe.

One concern is that the intermediaries, such as Google and others, are being handed either quasi-legislative or quasi-judicial powers to decide what is or is not being removed from what is almost a utility. Google is now used as a verb. If something is not there, it tends to be considered not to exist. People don't go to page 12 or page 112 to try to find some report on this. They play an important role, but they shouldn't be handed the authority to determine this. That's one consideration.

We do have others, but we want to make sure that if something is removed there's some sort of notation, some some sort of indication that what you're getting.... When you look something up, you're assuming you're getting what is there. If things have been removed —and I'm afraid I can't provide you with a detailed description of what that would look like—there should be an indication that what you're getting as a result of this search is not everything, if this is a road we are heading down.

● (1700)

Mr. Matt Jeneroux: Ms. Steeves.

Dr. Valerie Steeves: My colleague Jacquelyn Burkell at Western said it shouldn't be a right to be forgotten but a right to forget. We all do this. We all reinvent ourselves. We all go through experiences that we wouldn't necessarily want thrown back at us later on. I think that the right to be forgotten, as it's been articulated in Europe, is really about ease of access, especially if there's a public benefit to having that ease of access. Then that's part of the balancing. But even if you look at court records, court records have to be public because justice has to be public. It has to be seen as having been done. But when they started putting up matrimonial matters, and neighbours were looking up neighbour to see how much somebody made, it created all sorts of problems, so they took that off the Internet. It's still public; it's still available. That ease of access is what was causing the problem.

I think the potential with the right to be forgotten is that it's talking about that ease of access. Google is not a library. It's not the way we find everything. When there's publicly valuable information, you can still have journalists access that information at courthouses and through other investigative means. Just to build on what you were saying, to a certain extent it addresses the fact that we're relying on these tech companies to be curators, librarians, or journalists. If you look at the fake news crisis we're in right now, they're not journalists. We're realizing that there's a value in a democracy in having people who look at information and collect it for particular purposes, and companies are not playing that role. It's not even something they can do.

I think the challenge here is thinking of new ways to allow us as a democracy to curate information so we can create the privacy that individual citizens need to live their lives, but at the same time allow public debate to be nourished and enriched by good, curated investigative journalism and other sources of information like that.

Mr. Matt Jeneroux: That's excellent.

I have about 45 seconds left.

Quickly, Mr. Gogolek, under PIPEDA, do you find there's enough on child protection? The Privacy Commissioner said there is. We've heard another public interest advocacy group saying there's not. Do you think there needs to be a separate stand-alone piece on that, recognizing the provincial jurisdiction on a lot of that?

● (1705)

The Chair: You have 15 seconds or less.

Mr. Vincent Gogolek: It's a very complicated question. There is a jurisdictional question. I think we would probably be more comfortable dealing with the consent issue straight up, whether children of a certain age are able to provide it, rather than dividing them off from the rest of us [*Inaudible—Editor*]?

The Chair: Thank you very much.

Mr. Cullen, go ahead, please, for seven minutes.

Mr. Nathan Cullen: Thank you very much.

Thank you for the testimony.

Ms. Steeves, I want to pick up on the recent Federal Court decision with respect to the right to forget. Court cases were being posted on a foreign website, which then made them searchable so you could type in your neighbour's name and find out all sorts of things. Have we started down the road of the right to forget or the right to be forgotten?

Dr. Valerie Steeves: My colleague Michael Geist has argued that it is a foot in the door and that we're moving in that direction.

Mr. Nathan Cullen: Do you feel the same way?

Dr. Valerie Steeves: It's a de-linking kind of thing. To me, with the CanLII thing, it's closer to the way courts responded to their actual paper copies of records, so it seems to me that we're not quite there yet. I think it's something that would best be articulated by a thoughtful piece of legislation.

Mr. Nathan Cullen: Legislation....

You've suggested that journalists or librarians are the arbitrators of what becomes searched, of what is searchable.

Dr. Valerie Steeves: They're not the arbitrators but the curators. Those are different.

Mr. Nathan Cullen: Well, being a curator means having a great deal of power in someone's hands. That's to say that we're going to allow them to organize the information, and that what becomes searchable and accessible will be in their hands. Who plays that role? It's certainly not the Privacy Commissioner, and it's certainly not Parliament.

Dr. Valerie Steeves: Well, right now we're letting it be Google—

Mr. Nathan Cullen: That's right.

Dr. Valerie Steeves: —and I'm suggesting that when it's in the hands of librarians, there's a variety of different types of libraries, and there are stores I can go to if I want to access information. Similarly, with journalism, there is a broad range of different kinds of news outlets that we can rely on to feed that public debate.

Mr. Nathan Cullen: I acknowledge the problem we have with Google being the one demonstrating that, with the profit motive they may have and their organizing of things in the way that is most beneficial to them, yet I'm not sure that I'm satisfied with the alternative solutions you've offered, that librarians writ large or a store that I go into.... I think finding that out would help articulate what that thoughtful piece of legislation would look like in terms of the way we curate such private and personal information.

As for the right to forget, I thank God every day that I didn't have social media when I was a kid. I'm not going to tell you why, but I don't think I could have been elected if everything had been posted, and I think that may apply to some other colleagues around the table too.

I'll tell you later, Chair.

Voices: Oh, oh!

Mr. Nathan Cullen: My time is short, Mr. Gogolek. I assume you're referencing the B.C. PharmaNet breach today, in which 7,500 British Columbians had their personal medical information leaked—including for some of them, all of their medications and their medication history—by the net that tracks and tries to share information among pharmacists, which is a noble thing, because we want pharmacists to be able to track for all sorts of good public health reasons. I understand that the government knew about this last fall and that it's coming to light only today. How does the privacy law in B.C. or what happens federally not impact this decision by a government or a government agency that knew about a breach involving something so personal not to release that information for months and months?

Mr. Vincent Gogolek: This is one of the lacunae we have here in British Columbia, where PIPEDA actually has been updated to provide for breach notification. Here in B.C., we've had recommendations for this going back two years, and the provincial government has, for reasons best known to itself, decided not to act on this.

Mr. Nathan Cullen: What is the breach notification right now in B.C. and what should it be federally?

Mr. Vincent Gogolek: Federally, we would be looking for something stronger than what's currently in PIPEDA, but of course there is breach notification right now as a result of Bill S-4 from the last Parliament.

Mr. Nathan Cullen: Just to be very clear, when a breach happens, what is the law in British Columbia right now in terms of when notification has to be given?

Mr. Vincent Gogolek: Do you mean by the public sector?

Mr. Nathan Cullen: Yes.

Mr. Vincent Gogolek: I don't think there is one.

Mr. Nathan Cullen: Okay. Maybe that's a problem to be identified. I mean, if personal medical records have been breached—

Mr. Vincent Gogolek: Yes.

Mr. Nathan Cullen: —and people's medical histories are in the hands of God knows who and they may be shared or sold or whatever, the fact is that the government can choose not to tell anyone about it.

● (1710)

Mr. Vincent Gogolek: Well, this is the problem, but of course this is a provincial issue.

There's also the question, and this is something that's come up here, of what happens to the people who are, let's say, in danger of ID theft. Should there be a requirement that all the money that they'll have to pay to EQUIS, to TransUnion, or to the others—

Mr. Nathan Cullen: I'm just trying to understand the role of government with something like PharmaNet. They hold themselves apart from government; they are not part of government, and yet the Government of British Columbia—or nationally, if we're doing PIPEDA—sets the rules regarding, when a breach happens, when a company with something like personal medical information has to tell the public that this has happened.

You're suggesting that there isn't a breach notification.

Mr. Vincent Gogolek: It's not mandatory.

Mr. Nathan Cullen: It's not mandatory.

I have a quick question for either of our witnesses. It's about political parties and the information that political parties gather. What governs us right now federally in terms of how that data is managed and how the personal collection of private information of Canadian citizens is disclosed to those we're collecting the information from?

Mr. Vincent Gogolek: You're free to do with it as you see fit. You are not subject to PIPEDA. You're not covered there.

Mr. Nathan Cullen: Should this be changed?

Mr. Vincent Gogolek: It can and should be changed.

Mr. Nathan Cullen: Would you agree, Ms. Steeves?

Dr. Valerie Steeves: I would agree, yes.

Mr. Vincent Gogolek: In British Columbia the parties are covered. There's an argument that possibly federal parties that have B.C.-incorporated branches would be subject to the provincial legislation. It would create an interesting situation in which, if the federal party generally violates privacy norms, somebody in British Columbia would have the ability to file a complaint with our commissioner, but somebody in Ontario who's under PIPEDA would not. That seems unfortunate, to say the least, and it should be changed.

The Chair: Thank you very much.

We will now go to Monsieur Dubourg for seven minutes, please.

[*Translation*]

Mr. Emmanuel Dubourg (Bourassa, Lib.): Thank you, Mr. Chair.

First, I would first to thank the witnesses, Ms. Steeves and Mr. Gogolek, for being here. Your testimony is of great interest to the committee.

My first question is for Mr. Gogolek, since he is in Vancouver, very far away from us.

Did you know that the Quebec government conducted an awareness tour among high school students? Have you done anything similar where you are?

Mr. Vincent Gogolek: I am not aware of what is happening in Quebec. In British Columbia, our commissioner's office has produced resources to help people better manage their personal information, for young people and the general public. We also want to inform them of their rights and provide advice on protecting themselves and how to conduct themselves on the Internet and in other contexts.

Mr. Emmanuel Dubourg: Okay. I understand that awareness measures are ongoing.

You also stated that consent is an important issue and that is a priority for you.

Do you think there should be a time limit on consent? Do you think that would be helpful?

Mr. Vincent Gogolek: I think so.

Of course, it is up to legislators to draft the laws and find ways of achieving the intended purpose. I do not have a specific recommendation regarding a time limit on retention, but, in principle, consent should not be indefinite. Information should not be kept just in case it is needed at some undetermined point in the future. Consent should be used for clear purposes, and a time limit on retention should reflect that principle.

● (1715)

Mr. Emmanuel Dubourg: Okay, thank you.

Ms. Steeves, you talked a lot about children, and I do find it very worrisome that what our young people—who can be very young, as my colleague said—publish on Facebook or any other medium can catch up with them a few years later.

You also said that the legislation in Europe is much stronger, even better than what we have in Canada.

In your opinion, is the legislation in Europe much stricter as regards children than Canadian laws, PIPEDA for instance?

[*English*]

Dr. Valerie Steeves: If you look at both the EC and the EU, they've actually undertaken a number of studies recently that have expressly rooted privacy for children in the Convention on the Rights of the Child, even if you look at something like cyber-bullying where, in the Canadian context, we've been far too ready to invade children's privacy in order to protect them. Because of this commitment to the Convention on the Rights of the Child, the European discussion is much more about balancing the need to protect with the benefits of ensuring that young people have privacy in online spaces precisely because privacy is a proto-right. It allows them to access information, learn about their own culture, and these other things. I think there are some really interesting models there.

[*Translation*]

Mr. Emmanuel Dubourg: Okay.

Moreover, European legislation includes sanctions, which is not the case in Canada.

In your opinion, should we also impose sanctions, especially in the case of the fraudulent use of personal information?

[*English*]

Dr. Valerie Steeves: Do you mean fraudulent use among children?

Mr. Emmanuel Dubourg: Among everyone, I would say.

Dr. Valerie Steeves: That's interesting. I think part of the problem is that, from young people's point of view, when we create those kinds of remedies, they are less likely to use them. What they're looking for is more control over their information. So even again, when you look at cyber-bullying as an example and the zero-tolerance policies that have these penalties attached to them, if someone posts something about me that falls into this catchment.... Young people tell us that the problem with that is that if they go to adults, it gets escalated all the way, and then suddenly they lose control, and what they really want is an ability to get that information taken down. They want better mechanisms to be able to report information and say, “That's about me, and I want it removed.”

[*Translation*]

Mr. Emmanuel Dubourg: I have one last question for you.

You talked a lot about transparency as regards algorithms, stating in particular that this approach should be reviewed.

What are your thoughts on that? How should we review those algorithms? Should we also impose sanctions on people who use personal information in ambiguous situations?

[*English*]

Dr. Valerie Steeves: I'd refer you to the statement that's been put together by the Electronic Privacy and Information Center. They have an interesting statement of rights when it comes to algorithmic transparency. In a lot of ways, it's already in our legislation. They have to tell us what they're doing. They have to tell us why they're doing it. They have to tell us what the outcomes are. It's just that so often it's been buried in the algorithm in ways that make it even less transparent, so certainly a number of us within the civil society sector are quite concerned about this and think that it's worth pursuing as a provision in its own right.

A lot of it, too, requires that corporations be much more responsible for the outcomes. Yes, I do think there should be penalties attached when there are discriminatory outcomes in particular, and I think that would create a situation in which people would be much more careful when they are running algorithms that really significantly change people's life outcomes.

● (1720)

The Chair: That's interesting.

Thank you very much.

We have time for two folks in the five-minute round.

We'll go to Mr. Kelly and then to Mr. Saini, so let's keep it within our five minutes, colleagues.

Mr. Kelly.

Mr. Pat Kelly: Thank you, Mr. Chair.

So far, most of our testimony in this session seems, at its premise, to have been geared toward the larger businesses, the global social media players, such as Facebook and Google. I haven't heard Facebook named very many times, but I get the feeling that's who we're talking about in much of this. Yet this act in concert with provincial private sector privacy law, where it exists, is one that governs all businesses in Canada.

I'll ask both witnesses this. How well do you think all organizations that are subject to this law understand their obligations? We had Gary Dickson, the former Saskatchewan privacy commissioner, talking about doing audits or investigating compliance, and he found very little awareness regarding organizations' obligations under PIPEDA.

Dr. Valerie Steeves: And that certainly has also been found in studies that have been done by CPIC, for example. Andrew Clement has found the same in work he has done at U of T. So from what we can tell from the research, compliance is quite low.

In work I've done, what companies have said has been interesting. Again, it's, “I have a right to the information. The person has to give it because there's legislation.” So I think there is a very important piece with education, especially for small businesses. I know the commissioner has some material on his site that attempts to fill that void, but we have a lot of work to do in that regard, for sure.

Mr. Pat Kelly: We didn't get far in our testimony regarding what harm may have been done as a result of non-compliance. One thing they may have found going into a small business is that the proprietor is not aware of the obligations and hasn't undertaken certain obligations such as appointing a privacy officer, and these kinds of things. But where have we found harm? Which types of businesses are harming the public through their non-compliance with PIPEDA?

Dr. Valerie Steeves: In any complaints-driven process, you're going to find out what's going on only when someone is angry enough to complain. So as the tip of the iceberg, certainly the free flow of health information has created a certain number of complaints. As it moves from private sector legislation to public sector legislation, people are really concerned about that and when they find out that people have access to that, they're motivated to complain.

Am I going to be as worried if my bowling alley has collected that information about me? Again, its ability to collect is at this point limited by the nature of the business and the technology and the resources that it can bring to bear. I think that's why you've seen the main complaints about these larger issues with these larger companies. They're simply more visible.

Mr. Pat Kelly: I'm going to ask Mr. Gogolek to comment in the remaining time I have.

Mr. Vincent Gogolek: We'll probably be finding out more about what's happening here in B.C., where we apparently have the problem that Professor Steeves was talking about, with doctors' offices and PharmaNet being under our private sector PIPEDA-equivalent law. There are going to be questions about what's going on here and who fell down on this. There were a few doctors' offices involved, four I believe. I would suggest that we keep an eye on the situation here in British Columbia for an idea of how badly things can go wrong.

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

Mr. Saini, go ahead, please.

Mr. Raj Saini: I'm going to have two questions, but I want to sort of finish off on one question. We spoke about the right to be forgotten, and other people have mentioned minors and you also mentioned minors. As we explore the right to be forgotten, do you think there should be a special provision as a recommendation for those minors who may have given consent at a certain age? Do you think there should be a specific provision for them to have it totally eliminated?

● (1725)

Dr. Valerie Steeves: Yes, whether it's 18 or not. I think with anything before age 18, you should be able to get a clean slate and make it all just go away.

Mr. Raj Saini: I suggested that because you mentioned it in your preamble.

If you remember the case in Spain with Google, there were two provisions there. One was that the search engine could not provide a link to the information, but the link was being held by a newspaper that had been archived, so although it may not have been ubiquitous, it was still able to be found. Technologically, in what way can we do that? Is there some way?

Dr. Valerie Steeves: Again, it speaks to the earlier comment. It's the kind of remedy that would work well with social media, for example. I would know where my information was because I gave it to that particular organization.

Information about me that floats around is typically only brought to light when it harms me in some way, and then the remedy that most young people want is the ability to have it taken off of someone else's social-media account. It really reflects the ways that young people gather in particular places. Social media is a hot spot.

Education is another area of concern, because there are a number of companies that are now collecting minute details of young people's learning and commodifying it.

It was interesting—we started to try to look at political economy in both of these areas. One of the reasons we talk a lot about the big guys is that they buy the little guys. As soon as there's an information platform that attracts a lot of information and that becomes very marketable, it's bought by someone larger. Again, you see those honey pots. If we could address those honey pots, I think that would help.

Mr. Raj Saini: Mr. Gogolek, do you have any comments?

Mr. Vincent Gogolek: I think I'll pass on this one.

Mr. Raj Saini: Okay.

Do I have some time, Chair?

The Chair: Yes, you do.

Mr. Raj Saini: I'm going to ask you a technical question. It relates to a certain section of PIPEDA.

There are two things I want clarification on.

First, can you explain to me the difference between destroying data and making it anonymous?

Second, do you think that providing choice in the legislation creates a loophole?

Dr. Valerie Steeves: Those are good questions.

It seems to me that destroying data means magnetizing it, making it go away so that it's no longer held at all.

I am very skeptical about the ability to anonymize data, and I think the loophole it creates is this space for de-identified or anonymized data, which can be so easily re-identified, with so few factors taken into account. It goes back to the notion of retention as well.

The intention always was, “Tell me why you want it. I'll say yes. Once you're done, make it go away.” Yet, because of the monetary value of all this information, we're just letting companies hold it in perpetuity.

I think it is a loophole. It's another loophole that allows them to hold it because it might be valuable in the future.

Mr. Raj Saini: Thank you.

The Chair: Thank you very much. We have a minute left.

Ms. Steeves, in your opening remarks you mentioned something that caught my attention and I wrote it down. I don't know if anybody asked a question directly about it.

Could you elaborate and expand a bit more on the perception that younger people have insofar as audience control goes?

Dr. Valerie Steeves: Okay.

Typically, as I said, in a regulatory regime, we figure that if someone discloses something then it's no longer private, whereas their notion of privacy is relational, and they want to negotiate it with different audiences.

If I post something on my Instagram account, and that account is for my friends, I don't want my mother looking at it. I want a mechanism that will say, “No, that's not my family account. That's my friend account.”

Typically, when they worry about privacy invasions, it's because the barriers between their different audiences have been removed. This is all taken out of the social-media world and made accessible to anyone outside of those audiences, and there are harms to them because of it.

Two 13-year-old kids in Toronto went on vacation. They got back. They were talking about their tans online. One said, “I'm darker than you,” and they were called into the principal's office for racist bullying, because they both happened to be African-Canadian kids.

They were thinking, “I'm talking to my friends, and we're having a chat, but because this information can then be captured, now I'm under surveillance by my school and I'm accountable to my school for everything I say.” It's the ability to keep those lines firmly in place that they care about.

● (1730)

The Chair: Thank you very much.

Thank you very much, colleagues.

Mr. Gogolek, I think we kept you within your time limit, so I hope you'll be able to do what you need to do.

We thank you both very much for coming before the committee.

Colleagues, we'll see you here Tuesday of next week.

The meeting is adjourned.