HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 147 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, May 7, 2019

Chair

Mr. Bob Zimmer

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, May 7, 2019

● (1530)

[*English*]

The Vice-Chair (Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.)): Thank you for coming today.

We have a couple of different things to deal with today, including the estimates and a discussion about the joint investigation into Facebook and the Cambridge Analytica matter.

Mr. Angus.

Mr. Charlie Angus (Timmins—James Bay, NDP): Just before we get started, I want to give the committee notice that I will be bringing forward a motion for us to discuss a possible summons of Ms. Sandberg and Mr. Zuckerberg from Facebook.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thank you, Mr. Angus.

With that, we'll have opening comments from our Privacy Commissioner.

[*Translation*]

Mr. Daniel Therrien (Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada): Good morning, Mr. Chair and members of the committee.

Thank you for the opportunity to appear before you to discuss the 2019-2020 main estimates.

With me today are Deputy Commissioner, Compliance, Brent Roman; Deputy Commissioner, Policy and Promotion, Gregory Smolynec; and Deputy Commissioner, Corporate Management, Daniel Nadeau.

In the time allocated, I will discuss some of our plans for the coming year and how we expect to make use of the new funding announced in the recent federal budget, which comes in recognition of growing demands on my office.

Our annual resources have been approximately $24 million in recent years. We hope to have your support in maintaining that funding.

We plan to use the additional resources to enhance our ability to deliver on our mandated obligations in the face of the exponential growth and complexity of the digital economy. Privacy issues are multiplying rapidly and often adversely affect Canadians' privacy. It has been an ongoing challenge to keep pace with those advancements and to protect Canadians in the way they deserve.

We require program integrity funding to enhance our capacity to protect the privacy rights of individuals and achieve meaningful results for Canadians.

Of course, we welcome the recent federal budget announcement of additional resources for my office as a positive step. It would allow us to take concrete steps towards implementing our proactive vision for privacy protection. I am using the conditional here because even though the federal budget has allocated sums to my office, we will only have access to those funds once Treasury Board has given its approval.

Part of the funding included in the federal budget is temporary, to help us deal with a backlog of complaints. While we have undertaken initiatives such as the increased use of early resolution and the revamping of our investigative processes, we have nevertheless struggled to respond to complaints in a timely manner.

We currently have a backlog of more than 300 complaints older than a year. The new funds would allow us to reduce the backlog to approximately 10% of its size by 2021. We would also be in a much better position to achieve our goal of meeting service standard targets in 75% of cases.

Ultimately, however, we think the best solution in the enforcement area is to modernize legislation, in part to give the OPC greater authority to manage its caseload according to risk. We need the discretion to focus our efforts on those cases with the greatest impact on Canadians.

The new funding will also be used to process privacy breach reports. Since mandatory breach reporting requirements came into effect in November 2018, our office has seen the volume of reports increase to more than five times what it was when reporting was voluntary. At present, we can only superficially respond to the vast majority of private sector breach reports to our office.

New resources would enable the OPC to more thoroughly review 40% of private sector breach reports to our office and 15% of public sector breach reports.

● (1535)

[*English*]

A third activity for which the federal budget provides additional funding is in the area of public education and guidance. The number of privacy issues for which parliamentarians, businesses and individuals require our advice and guidance is multiplying at a rapid pace.

In the past five years, requests for advice to Parliament have risen considerably, and this trend is expected to continue. Calls from various parliamentary committees are up 41% from five years ago, and in 2017-18 alone we made 34 parliamentary appearances and submissions. Clearly, privacy is becoming a very important issue for parliamentarians.

In the coming year, we will remain responsive to parliamentarians' requests for advice on the privacy implications of bills and studies, and we will seek to contribute to the adoption of laws that improve privacy protection.

New resources would also help increase our capacity to inform Canadians of privacy issues relevant to new technologies, their rights and how to exercise them. As well, we would be better positioned to guide organizations on how to meet their privacy obligations.

With current capacity, we can produce a maximum of three new pieces of guidance a year. Following our consent consultations a few years ago, we have developed an ambitious plan for much-needed guidance related to a wide range of important issues—guidance that we were asked by stakeholders to produce. Guidance to be developed over the next few years includes important issues such as biometrics, the Internet of Things, social media and de-identification, among others.

As well, existing advice and guidance needs to be updated to ensure that our website continues to be a trusted and comprehensive source for both organizations and individuals. There are over 150 guidance pieces on the OPC's website, approximately 40% of which are five years old or more.

Another important area for our office in providing guidance involves our advisory services to both industry and government. The new funding would help support our work with industry proactively in an advisory capacity to better understand, advise and help mitigate any privacy impacts at the design stage of their services.

Finally, I would add that guidance needs to be complemented by sustained and effective communication and outreach to have meaningful or significant impact on awareness and understanding of rights and obligations. We would therefore like to increase our capacity to conduct more public education and outreach activities to have a greater impact on awareness and understanding of privacy rights and obligations.

Of course, as you've heard me say before, our federal privacy laws require a number of very urgent reforms. As our recent Facebook investigation so starkly illustrated, we have reached a critical tipping point upon which privacy rights and democratic values are at stake.

I look forward to discussing those issues in an hour or so.

In conclusion, keeping pace with the rapid changes in technology is going to be an ongoing challenge for our office. We will continue to make optimal use of the resources given to us to carry out our mandate to have a greater impact on the privacy rights of Canadians. The recently announced new funding is an important interim measure and positive step towards achieving our targets as we await much needed legislative modernization.

Thank you, Mr. Chair. My colleagues and I look forward to your questions.

● (1540)

The Chair (Mr. Bob Zimmer (Prince George—Peace River—Northern Rockies, CPC)): Thank you once again, Commissioner. I just wanted to give you a heads-up from the committee. I think it's been discussed amongst parties and members that we'll have one seven-minute round per party and then we're going to get right into the Facebook report, if that's okay with you.

Mr. Daniel Therrien: Sure.

The Chair: We'll start the first seven-minute round with Mr. Saini.

Mr. Raj Saini (Kitchener Centre, Lib.): Good afternoon, gentlemen. Thank you so much for coming.

Mr. Therrien, I read the report here, which is your departmental plan for 2019-20. I just had a few questions on it, for clarity.

One thing was that there was a decrease here. Under departmental results and “Privacy rights are respected and obligations are met”, the target percentage of complaints responded to within service standards is 75%, but it's been going down. It was 68% in 2015-16, 55% in 2016-17 and 54% in 2017-18.

Is there a reason that's happening?

Mr. Daniel Therrien: I think a major factor is the complexity of the issues that we are investigating. Often, they involve fairly complex technological issues, business models and technology. We have experts to carry on these investigations, but they are becoming more complex and that takes time.

Mr. Raj Saini: When I look at some of the charts here, it says that the information is not available. Is that because you've only recently started to collect data?

If you look at the next lines, which are “Percentage of informal OPC recommendations”, “Percentage of Canadians who feel they know about their privacy rights“ and “Percentage of key privacy issues”.... Is it because you've just recently started to collect that?

Mr. Daniel Therrien: It's because the the departmental results framework is new. The government has adopted a new policy on how to describe results for parliamentarians and that's what we have done. We are in the first year of the implementation of that process.

Mr. Raj Saini: Okay.

The amount of money you've asked for has gone up by about $5 million, if I'm right, from the previous year. Now, as I read the report, you have now a mandatory breach reporting provision. Has that caused this increase, this backlog, because now, rather than voluntarily, people or organizations have to mandatorily—

Mr. Daniel Therrien: It's one of the reasons that we're facing a higher volume. In particular, if you look only at breach notifications, previous to November, organizations could voluntarily report; now they have to when there's a material breach. The volume of these reports has increased fivefold since November. That's clearly a reason for the increased volume. It's not the only one, but it's an important one.

Mr. Raj Saini: With regard to the increased funding you've asked for, I see here that you have planned to keep the human resources or full-time equivalents the same. Would you not need to hire more people to deal with the backlog?

Mr. Daniel Therrien: We will. Currently, we have roughly 180 FTEs. We have around 195 individuals, but not all of them work full time. With the new funding, we will likely hire roughly 30 more people.

Mr. Raj Saini: Okay.

As you know, obviously, the last time you came here you gave us an update on your inquiry into Facebook. That inquiry itself must have consumed a lot of resources. Did you apply the same resources to that issue or more resources to that issue?

Mr. Daniel Therrien: We clearly applied more resources to that investigation than to an average investigation.

Mr. Raj Saini: Did that cause other things to sort of slip behind?

Mr. Daniel Therrien: Yes. There was not only Facebook. Facebook was a very important investigation in the past year, but Equifax was also an important investigation, and there were a few others. We need to look at these issues thoroughly. They affect a large number of Canadians. That's the result.

● (1545)

Mr. Raj Saini: Thank you.

I'll pass the rest of my time to Mr. Erskine-Smith.

Mr. Nathaniel Erskine-Smith: I have just one question. You spoke about the rapid advance of technological change and seeing more resources spent in the last year on larger investigations. You mentioned a couple of them just now. When you look ahead—you see an increase in resources in this past budget, and I know you welcome that—is there a number that you would suggest this committee recommend to government to say, “If we receive this amount, we could accommodate the existing caseload and we would also be able to accommodate what we expect to be the workload going forward”?

Mr. Daniel Therrien: In terms of the volume of complaints, I see the federal budget as bridge financing, allowing the OPC to function and to dramatically decrease the backlog in the next two years or so. My hope, certainly, is that by that time, there will be new legislation. It's a bit premature to say at this point how many resources would be required to implement a new system that has not yet been defined.

Mr. Nathaniel Erskine-Smith: That's fair.

Thanks.

The Chair: Mr. Gourde, go ahead for seven minutes.

[*Translation*]

Mr. Jacques Gourde (Lévis—Lotbinière, CPC): Thank you, Mr Chair.

Commissioner, thank you for being here this morning. My colleagues were very inspired and they asked several of my questions.

From an optimistic perspective, given the increase in the number of complaints, do you think you will be able to stabilize the OPC budget, or should we expect these additional amounts to become permanent over the next three or four years?

Mr. Daniel Therrien: As for the complaints as such, as I explained, the budget should allow us to eliminate most if not all of the current backlog. We expect to reach a point of equilibrium within two years if the number of complaints and their complexity remains about the same.

I am hopeful that new private and public sector laws will have been adopted in the next two or three years. We will be able to assess the resources that are needed to process the complaints filed under those new laws once we know the tenor of the legislation and the responsibilities they bring.

In short, I think that the funding allocated to us in the budget, if it is confirmed by Treasury Board, will allow us to manage our backlog by the time the new law is implemented in two or three years.

Mr. Jacques Gourde: In your presentation you mentioned that the number of complaints had increased fivefold. Was there a triggering element? Are the new complaints like the others, or are they more varied?

Mr. Daniel Therrien: It is, more specifically, the number of privacy breach reports that has gone up by a factor of five. That increase is attributable to the coming into effect, on November 1, 2018, of regulation obliging companies to disclose any important privacy breach.

The number of regular investigations following complaints of violations of the Personal Information Protection and Electronic Documents Act, which applies to private sector organizations, has not increased as much.

Now that that regulation is in effect, the annual number of reports should ultimately stabilize over the years.

Mr. Jacques Gourde: We are holding back the questions we'd like to ask on Facebook because we will be getting back to that file later.

Is it your opinion, however, that Canadians are more worried about the protection of their privacy now than before? The Facebook issue seems to have made people more aware of this reality. Is that true? Have you noticed a difference?

● (1550)

Mr. Daniel Therrien: Surveys show that the level of concern has always been quite high. That said, I think that Canadians and people throughout the world have indeed become more concerned over these past years.

The Facebook and Cambridge Analytica affair certainly played a role in that. That serious incident showed that the consequences of privacy breaches were not just theoretical, but could be quite concrete. In this case, the integrity of the electoral process was affected.

The protection of privacy and personal information is a notion that can be relatively theoretical and abstract. But in the Cambridge Analytica case the results were very concrete, and that increased Canadians' level of concern.

Mr. Jacques Gourde: Thank you, Mr. Therrien.

We will get back to Facebook later.

Mr. Daniel Therrien: Of course, Mr. Gourde.

[*English*]

The Chair: Thank you.

Next up, for seven minutes, is Mr. Angus.

Mr. Charlie Angus: Thank you, Mr. Chair.

Thank you, Mr. Therrien, for coming before us.

You will be going to Federal Court with one of the most powerful corporations in the world. I think the maximum Canadian fine is something that I was told Facebook makes in about 60 seconds. Facebook is going to want to spend whatever it takes to defeat you in court.

In your legal presentation, will you have to be drawing on your existing budget, or will the justice department cover the extra costs of ensuring the people of Canada are well represented in court?

Mr. Daniel Therrien: We will pay for our legal costs and fees through our budget. We have a team of lawyers, some of whom plead, but we often rely on outside counsel as well, for cases in the Supreme Court, for instance. This is a very important case, and I will draw on our budget to be successful. My intent, obviously, is to be successful, and to have the court declare that Facebook violated PIPEDA. The company has treated our findings as a legal opinion. They will not be able to ignore the findings of the Federal Court, and the court's order will be binding on Facebook.

You might say that the fine will be inconsequential. Perhaps it will be, but there will be an order, we hope, at the end of that process, and that order cannot be ignored. There might be consequences other than monetary to disobeying a court order.

Mr. Charlie Angus: My concern is in making sure that you have the resources. I've been on this beat for about eight years, and the various offices of Parliament come before us and talk budgets. There are always constraints and limitations, but in your office, it seems to me, the mandate is changing—it's dramatically different. The Commissioner of Lobbying has always dealt with dodgy questions of lobbying here and there; the Ethics Commissioner deals with what is dealt with there. I have nothing against their work. It's very important work, but it would seem to me that.... This office was created in 1977. The Privacy Act was passed in 1983 for the public sector, and then PIPEDA was passed in 2000.

When I came on this file, your office would be dealing with lost hard drives and USB sticks, and the breaches tended to be corporate mistakes. These were questions of corporate governance, the lack of protocols in the office. What we're dealing with is the emergence of surveillance capitalism, and it's a very different beast, where there's a direct corporate interference in the lives of citizens, which is profoundly undemocratic, by companies that have enormous powers.

I'm getting to my point in a roundabout way. Is your role transforming from a regulator to an investigator? If that is the case, should we be rethinking how the office works and what your tools are? To ensure the privacy rights of Canadians in this world that is emerging around us, are the old tools sufficient?

Mr. Daniel Therrien: They're clearly not sufficient. I've said this a number of times. I think Facebook is a perfect illustration of the fact that the current tools that we have are insufficient. I cannot make binding orders, contrary to many other data protection authorities across the world, but I can bring them to court. One could be concerned about whether we have sufficient resources to fight equally with a company that size in court. It's fair question, but the federal budget has reserved not inconsequential sums of money for us. I will use them, and the Facebook Federal Court matter will be a priority. If I see that I need more resources to have success, I will not hesitate to ask this committee, Parliament and the government for additional funds. We're not there yet.

● (1555)

Mr. Charlie Angus: Right.

I think what really surprised our committee when we started to delve into this case with the Cambridge Analytica scandal was how complex it was, how difficult it was for our parliamentary committee to get answers. You're dealing with, basically, dark data by people who work in a very different realm from ours in what we do as legislators.

Christopher Wylie had stated that he felt that the U.K. ICO was very unprepared when it came to taking on Cambridge Analytica, because it did not have the experience of knowing how these players operated. Fortunately, the ICO in the U.K. did an excellent report.

Putting it to you, in terms of the changing world we're dealing with of surveillance capitalism and particularly data mercenaries, some of whom we brought here, do you have the resources that are necessary to actually be able to play in that milieu, of having the technical people, the people who know how the hard drives are being misused, how data's being moved around? It's in a very different realm than anything we've dealt with in the past.

Mr. Daniel Therrien: I approached this incrementally.

The first point of order is that the law needs to change so that we have the right tools, the right legal tools, to ensure compliance by corporations. That won't happen immediately, but my hope is certainly that within a very few years this will happen. Then, at that point, there needs to be a discussion around the resources necessary to make that system work.

With the sums reserved for us in the federal budget, I think there's a.... I asked for more, but we received a not inconsequential sum of money to bridge us toward this new legislation, which I hope will be adopted within a couple of years. I'm fairly optimistic.

Do we have all of the tools we need, including resources? No, and choices have to be made. You're right to point out that, as with any other regulator, because of the exponential changes to technology and the digital economy, we have many issues and companies to monitor and look at, and we need to make choices. We cannot go after all problems—even serious—but the resources that were given in the budget will certainly make an important difference. Let's have a discussion around what the shape of the new legislation should look like, and then we can talk about the necessary resources.

As a comparator, I would say that with the new funding our size would be similar to that of large European data protection authorities, but much smaller than the U.K. Information Commissioner's Office. What is the right size is a question for discussion.

The Chair: Thank you.

We'll move into the second part of our meeting, pursuant to Standing Order 108(3)(h), on the study of a joint investigation of Facebook Incorporated by the Privacy Commissioner of Canada and the Information and the Privacy Commissioner for British Columbia.

We again have with us Commissioner Therrien. We also have with us Brent Homan, deputy commissioner, compliance sector.

Go ahead for 10 minutes.

● (1600)

Mr. Daniel Therrien: Thank you.

You have a statement from me on Facebook. I'll use it liberally.

[*Translation*]

As to the conclusions of our study, we found that Facebook violated privacy on a number of counts, including the rules on obtaining meaningful consent.

We studied two groups of Facebook users. The first was made up of users who installed third-party apps. As far as they were concerned, Facebook counted on the privacy policies of app developers to see to it that users' privacy would be respected. However, when we dug a little to see if those policies had any substance, we found that Facebook did not in fact verify whether app developer policies protected privacy properly. That is one example we found of Facebook's lack of responsibility.

Facebook has direct obligations under PIPEDA, the Personal Information Protection and Electronic Documents Act. When that company discloses information to a third party application, it is unacceptable that Facebook counts on the other company's privacy policies to respect its own obligations, which are independent. There is, consequently, a breach of privacy in that instance.

The other type of user we studied included the friends of Facebook users who installed third-party apps. When people joined Facebook, according to Facebook, they consented to the disclosure of their own information when friends installed third-party apps. The friend of the user was thus considered, according to Facebook, to have given consent to some unknown action that could take place years later, for unknown purposes. That is the very opposite of informed consent. One of our conclusions was that informed consent was not obtained.

Ultimately, our final conclusion was that Facebook breached one of the PIPEDA principles, which is that companies that collect and use personal information are responsible for the management of that information. We feel Facebook's main transgression is that it shifted its responsibility onto the users or the third-party app developers it dealt with.

Facebook even challenged our conclusions. Among other things, and in a fundamental way, it challenged our assertion that when a user uses a third-party app, Facebook discloses information to that app. According to Facebook, the transfer of information from Facebook to the third-party apps was not a disclosure on its part. It characterized this as making information available at the request of its users.

Once again, we see that Facebook is sloughing off its responsibilities. It claims that it is up to others to be careful, whereas we are of the opinion that Facebook has a legal responsibility to obtain informed consent if information is disclosed.

Among the matters we will be submitting to Federal Court is this fundamental issue: does the fact that Facebook transfers information to third-party apps constitute a disclosure under the law, or not? We believe it is quite clear that the answer to that question is yes.

● (1605)

Another thing I would insist on is the difference between Facebook's actions and its statements; it says that it wishes to adopt a position that is favourable to protecting privacy, and that it wants to work with governments and regulatory agencies to better protect the privacy of its users. All of that is good, but in reality, we saw exactly the opposite. Facebook stated that it wanted to work to further the respect of users' privacy with the regulatory agencies, and so on. However, we had some conclusions to present to it, and recommendations to ensure the company would comply with federal legislation. In the final analysis, the result of our discussions with Facebook, which lasted a few weeks, was that it rejected our legal conclusions as well as our recommendations.

That is exactly the opposite of the official position Facebook puts out, which is that it wants to work to ensure the protection of privacy with the regulatory bodies.

[*English*]

Very briefly, Facebook, in our view, violated PIPEDA with respect to consent. We think the main violation is with respect to its lack of accountability. PIPEDA's first principle is that companies have a legal obligation to be accountable for the way in which they handle the personal information of those from whom they collect information. They did not comply with that fundamental obligation. At the end of the day, they refused our findings, point one and point two, our recommendations. I think it is untenable that the law is such that this is our current state of affairs.

A company should not be able to say to a regulator, after the regulator has done serious work to look at the practices of the company, "Thank you very much, but we disagree. We don't think we are disclosing information to third party applications. We think they are making that information available at the request of our users, therefore we, Facebook, think that you're incorrectly applying PIPEDA."

It is completely unacceptable and untenable that as a regulator I am in that position and that my decisions are not binding on the company. That's the plea that I'm making to you. I know you have agreed with our office in the past that we need stronger enforcement powers to make sure that companies do comply with the law. I have to, in this forum, underline how unacceptable it is that we at the OPC are in that situation as we speak and that we have to go to court to ensure that this company is under an order to comply with the law.

The Chair: Thank you, Commissioner.

I will start off first of all with Mr. Erskine-Smith for seven minutes.

Mr. Nathaniel Erskine-Smith: Thanks very much, Commissioner, for the work of your office and the work of the B.C. commissioner's office.

I want to start by quoting Mr. Zuckerberg. Recently, at an F8 developers conference, he said:

> Now look, I get that a lot of people aren't sure that we're serious about this. I know that we don't exactly have the strongest reputation on privacy right now, to put it lightly. But I'm committed to doing this well.
>
> The future is private.

Then I read from your report, and you say:

> We are disappointed that Facebook either outright rejected, or refused to implement our recommendations in any manner acceptable to our Offices. This is particularly troubling given Facebook's public commitments to work with regulators and rectify the "breach of trust" associated with these events.

In a different part of the report, you say:

> We were disappointed that Facebook repeatedly failed to meet submission deadlines for the voluntary requests and provided incomplete or deficient responses to several of our questions, certain of which remain unanswered.

We have comments in your report and we have recent comments from Mr. Zuckerberg. Is there any reason to have confidence that Facebook is taking privacy seriously?

● (1610)

Mr. Daniel Therrien: We have not seen it in the context of the investigation we have concluded. They have told us publicly, "We want to work with you. Facebook wants to work with you, the regulator, OPC. Let's try to work together." At the end of the day, they reject the legal conclusion and the recommendations.

Mr. Nathaniel Erskine-Smith: When they have the opportunity to act consistently with the words they are providing to this committee and to your office, their actions fall well short of their words. Is that fair to say?

Mr. Daniel Therrien: Yes.

Mr. Nathaniel Erskine-Smith: We have the FTC talking about fining Facebook over breaches of privacy, and breach of a previous agreement with the FTC. Facebook has potentially set aside, ready to pay, $5 billion.

We have the U.K. Information Commissioner levying a 500,000-pound fine. She said, "We consider these contraventions to be so serious, we imposed the maximum penalty under the previous legislation. The fine would inevitably have been significantly higher under the GDPR." You are able to levy a fine in the amount of—

Mr. Daniel Therrien: I'm unable to levy any fine.

Mr. Nathaniel Erskine-Smith: Isn't that interesting?

Mr. Daniel Therrien: After being asked to review the matter *de novo*—not our report, but the matter *de novo*—the court could certainly make a declaration, if it agrees with our position that Facebook violated PIPEDA. There could be damages that historically, in the Federal Court, have been in the tens of thousands of dollars.

Mr. Nathaniel Erskine-Smith: Right, and a court would have to take it upon itself to levy significant punitive damages it's never awarded before, because there's not a strong statutory basis for doing so.

Mr. Daniel Therrien: Yes.

Mr. Nathaniel Erskine-Smith: You noted that Facebook's privacy protection framework was empty. That was then. They have taken some steps. Given that you don't have the powers to proactively audit, and they've refused to implement or agree to annual audits, are you able to realistically assess their current privacy framework?

Mr. Daniel Therrien: The comment that the privacy framework was empty still applies. It is empty.

I'll give you two examples. The comment actually refers to the previous investigation by the OPC, in 2009. My predecessors reviewed very similar issues, such as the consistency with PIPEDA of disclosure by Facebook to third party applications. The OPC found that this was done on the basis of vague terms and conditions that did not represent meaningful consent. Facebook, at the time, agreed to make certain changes to its procedures, and it didn't. "The framework is empty" is a comment about the framework adopted then.

Mr. Nathaniel Erskine-Smith: In light of that, does it make any sense at all that a company that has failed to respect Canadians' privacy rights would then be implementing a dating app on the service they're currently providing to Canadians? Does that many any sense at all to you?

Mr. Daniel Therrien: No.

Mr. Nathaniel Erskine-Smith: You don't have to go further on that. It just seems ludicrous.

You mentioned that the current laws are untenable. With the current state of affairs, I would completely agree with you.

It's interesting. I was in Brussels recently. I met with the EU data protection supervisor and other people thinking very seriously about privacy. They spoke very favourably of the ideas that have come out of Canada, both from Canadian privacy commissioners and from Canadian academics who have written about privacy. Their laws are based on our ideas, and our laws aren't based on our ideas. It seems an incredible shame.

Last June, I introduced Bill C-413. Had that bill been law, you would have been able to make orders. You would have been able to order Facebook to comply with your recommendations. You wouldn't have to seek the help of the Federal Court. Is that true?

Mr. Daniel Therrien: Yes.

Mr. Nathaniel Erskine-Smith: If that law had been in place at the time of the offence, you would, at the very least, be able to levy fines. Facebook would not be facing $5 billion in the U.S., 500,000 pounds in the U.K. and zero in Canada. There would be some monetary sanction we would be able to apply here. Is that fair?

● (1615)

Mr. Daniel Therrien: Yes.

Mr. Nathaniel Erskine-Smith: I have a last question. I think you'll agree with me that we've thought a lot about improving our privacy rules at this committee, and I think Canadians expect that we will have strong privacy rules in place. But if we don't have a strong regulator to enforce those rules, it doesn't seem to me that those privacy rules and the effort to strengthen the privacy rules are worth much at all. Is there anything as a first step that matters more than creating a strong privacy regulator here in Canada?

Mr. Daniel Therrien: I would say there are at least two important solutions. One is to make sure the regulator has the right powers, and in that basket would fall binding orders, penalties and proactive inspection powers that I've discussed in this committee before and can expand on if we have more time.

But I will move to another part of the solution, which I think is to ensure that we have rights-based legislation. Facebook and Cambridge Analytica demonstrated the link between privacy protection and the exercise of other fundamental rights, in this case democracy. But there's also a link between privacy protection and other fundamental rights: equality, for instance, in the employment context; freedom to go on the Internet to develop as a person and look for issues of interest without the fear of being monitored by corporations. A clear link was demonstrated in Cambridge Analytica, but it's just one example of the clear link between privacy protection and the exercise of fundamental rights.

I think this shows that, in addition to giving powers to the regulator, the new legislation has to be framed as perhaps principles-based, as PIPEDA is, but also rights-based, and recognize that privacy protection is linked to the exercise of other fundamental rights. We're all at risk if privacy is not protected. We would not only lose our privacy, but other rights would also be at risk.

Mr. Nathaniel Erskine-Smith: Thanks very much.

The Chair: Next up, for seven minutes, Monsieur Gourde.

[*Translation*]

Mr. Jacques Gourde: Thank you, Mr. Chair.

I have a more general question regarding the consent, of Canadians in this case, that is required by applications. On Facebook, a page appears and it says that in order to continue, you have to read what is written there and click on the "I accept" button to give consent.

Last week a witness told us that we should regulate that and that more information should be given to Canadians about the consent forms drafted by Facebook or third-party apps. By giving our consent, we are also giving it to apps that don't even exist yet.

Very often Canadians don't even read the conditions. They are in such a hurry to access the app that they accept automatically. Facebook's defence is that Canadians agreed and that this protects it.

Is there a better way to inform Canadians? When they click on the "Accept" button in an app, they are indeed entering into a type of contract. Is this type of acceptance that Facebook requires to protect itself against potential legal proceedings valid?

Mr. Daniel Therrien: In the course of an investigation, we examined Facebook's current policies. We concluded that that consent was not valid, because users were consenting to something that might only occur years later. Obviously, they can't know what will happen years later. Even if there is a lovely legal text that is 50 pages long, if it does not inform Canadians about the use that will be made of their information, that consent is not valid.

As you know, in January of this year, we published guidelines to get companies to develop clearer privacy policies. That is part of the solution, but it is not the whole solution. That is why I advocate the adoption of a privacy protection law that goes beyond important principles such as consent. Consent is important, but it does not solve everything. We need a law that defines privacy in sufficiently general terms.

Protecting one's privacy does not end with giving or withholding consent. Consent is a means. Having the right to privacy means being able to communicate with our friends on social media without worrying that some company is constantly monitoring our activities. Cambridge Analytica used our information to try to influence our political opinions and our vote. We have to define the right to privacy in a sufficiently general way, and that goes beyond consent.

I have before me a bill that was tabled in a previous Parliament. It defined the right to privacy, among other things, as the right to be free from all surveillance.

Any new law on the protection of privacy, in the public or private sectors, should begin with that. What is the right to privacy? Is it tied to the idea of granting consent? No, it is not limited to that. The right to privacy is the right to one's own physical privacy. It is the right to be free from all monitoring, the right to be free from having one's private communications intercepted by the state or by private companies. That is where the definition should lie. After that, procedures or mechanisms like giving consent come in to protect the respect of privacy, but protecting privacy is not limited to consent.

● (1620)

Mr. Jacques Gourde: Once such a law has been passed, we can develop the framework around consent and even impose it on Facebook, rather than having it foist fake consent on us. If consent were imposed and regulated by a Canadian law, don't you think Canadians would enjoy much better protection?

Mr. Daniel Therrien: The practical enforcement of these legal rules will be complicated, I can't deny that. However, if we define the right to privacy with the right level of generality and importance, we will never again be in the situation you've described a few minutes ago. At this time, a company can say that its contract informed the user that it would use their private information for certain reasons, that the user consented, and that it is behaving correctly and complying with the law.

If we had a rights-based law where consent was an important mechanism but not the ultimate purpose, and if a company's monitoring, as consensual as it may be, led to the monitoring of an individual's activities, the regulatory body would have the power to intervene because despite the consent, the substance of the right to privacy would not have been respected.

Mr. Jacques Gourde: Thank you.

[*English*]

The Chair: Mr. Angus, for seven minutes.

Mr. Charlie Angus: Thank you, Mr. Chair.

I want to say at the outset how important the work of your office is. For too many years, we've been played for suckers by Silicon Valley, that it was about choice, that it was opt-in, opt-out. We could read the privacy provisions. It never respected the privacy provisions in building its models.

What we've learned with Cambridge Analytica and Facebook is that this is not simply a question of the rights and the choices of consumers. This is about the democratic rights of citizens. It's about the questions of a nation state being able to actually ensure that its citizens can live in a world where they choose certain rights that are protected and inalienable, and one of those rights, as you said, is the right to be free from surveillance.

I want to start off with a few simple questions. Your finding was that Facebook broke the law of Canada with its breach of PIPEDA. Is that correct?

Mr. Daniel Therrien: That's correct.

Mr. Charlie Angus: As an officer of Parliament, you have been mandated to ensure compliance with PIPEDA. Was your report an opinion or is that a finding of fact by the officer in charge of representing the Parliament of Canada in preserving our laws?

Mr. Daniel Therrien: It's a finding of fact and law.

The statute under the current law is not binding on the corporation being monitored by this agency.

● (1625)

Mr. Charlie Angus: Facebook initially stated that you didn't have jurisdiction because you couldn't prove that the 620-some thousand Canadians who had their private information stolen were somehow affected. Didn't they then move on to say it was an opinion of yours and they'd take it under advisement? Where are they? Is this their opinion or that the fact that we don't have jurisdiction? What is Facebook's response to you on this?

Mr. Daniel Therrien: They raised the jurisdictional question. We've answered it in our report. They never acquiesced to our jurisdiction. They pursued a discussion with us as though we had jurisdiction but never conceded that we had jurisdiction. That's the state of affairs. If Facebook raises this issue in the Federal Court when we file our application, the court will decide whether we have jurisdiction.

Mr. Charlie Angus: When we began our hearings, and I first wrote to you, it was the spring of 2018 when the Cambridge Analytica scandal had just blown up and we had found that 620-some thousand Canadians had their information taken. Facebook was made aware of that in 2015 and made no effort to tell Canadians.

They said at the time when they came to our committee in 2018 that they had a very robust response. I'm flabbergasted that a company would look at a finding of law and say they simply don't recognize their jurisdiction.

Are you aware of other examples of companies saying that in Canada?

Mr. Daniel Therrien: I'm not. There may be other regulators that don't have the authority to make binding orders, but nothing comes to mind.

Mr. Charlie Angus: I was trying to think of a comparison. I was imagining when we have automobile recalls because of numerous accidents, that if an automobile company came back to you and said there are multiple accidents in Brazil, in the United States, in Britain, however, since you couldn't prove that anybody died on the highways of Canada, they don't recognize your role as a regulator to make them fix the fundamental problems in their vehicles.

I want you to correct me if I'm wrong, because they said it would cost too much for them to comply with the laws respecting the rights of Canadians.

Would that be a fair comparison?

Mr. Daniel Therrien: It's a good analogy. We were in discussions with them as to whether their privacy policies led to meaningful consent. They disagreed that they did not obtain meaningful consent but moreover, part of their arguments was, in any event, there was no harm. No Canadian was harmed.

You haven't found evidence that Canadians were harmed, which is a good analogy to your car accident example.

Because we did not demonstrate harm to Canadians, we have no jurisdiction. Point one, the legal foundation leading to risk and potential harm to Canadians we found was unsound, contrary to PIPEDA. Point two, we have seen harm in the U.S. and in the U.K. based on the same weak legal foundation. The same risk that manifested itself in the U.S. and the U.K. could very well occur in Canada.

We looked at the terms and conditions. Cambridge Analytica was one manifestation of one third party app. Facebook has millions of third party applications. Clearly, there is harm for Canadians.

Mr. Charlie Angus: I'm not a lawyer but I'm thinking the basic concept of jurisdiction—and correct me if I'm wrong—means the country of Canada for which you are a regulator, and 620-some thousand Canadians had their data taken because of this breach. Facebook was aware for it for three years and made no effort to tell Canadians. Within the jurisdiction of Canada, they broke the law because they did not make any efforts to let any Canadian know they had been a subject of this breach.

Is Facebook putting forward the position that jurisdiction only counts, only exists if you can prove that Facebook physically caused harm by its actions?

Mr. Daniel Therrien: It's pretty close to the position we heard from them. They're not challenging our jurisdiction on the basis that they're in the U.S. or anything of the kind. They're challenging our jurisdiction on the basis that the terms and conditions we were examining did not, in their view, result in harm, and the absence of harm led to the absence of jurisdiction. We think that we have jurisdiction because we have jurisdiction to look at what I call the legal foundation, i.e. terms and conditions—

● (1630)

Mr. Charlie Angus: You have jurisdiction because you're there to protect the rights of the citizens of our country as mandated by Parliament. Is that not how jurisdiction works, and your obligation is to protect our citizens whether—

Mr. Daniel Therrien: Facebook is engaged in commercial activity that is subject to PIPEDA, which gives us jurisdiction.

Mr. Charlie Angus: Thank you.

The Chair: Next up for seven minutes we have Monsieur Picard.

[*Translation*]

Mr. Michel Picard (Montarville, Lib.): Thank you.

Did you see the two-part documentary about Facebook?

I don't know if it was on HBO or the *Fifth Estate*.

Mr. Daniel Therrien: No. I'm sure my colleagues saw it, but I didn't.

Mr. Michel Picard: Fine.

Both parts of the documentary talk about fake news, as well as Cambridge Analytica.

Obviously, the questions that were put to Facebook's former executives give us to understand that there was extreme naïveté among all of the executives, so much so that no one was aware of consequences or of the legal repercussions of using the information they collected from people.

In parallel, one of the important defences Facebook used rested on the famous *Safe Harbor Rule* in America. In fact, under that rule, you cannot criticize a business for the type of actions we are discussing here, to the extent that the nature of the company means that it cannot be caught under the terms of the law.

Does that mean that the structure of Facebook or the nature of its activities allows it to take advantage of a type of legal void and consequently, to not get caught?

Otherwise, is that hypothesis not applicable because the company is defined like that, it has activities that are also defined a certain way, and it claims to be providing a given service?

Does that exclude it from any legal proceedings?

Mr. Daniel Therrien: The arguments about jurisdiction put forward by Facebook did not concern the territory, the location of the data on a given territory. The notion of *Safe Harbor* potentially calls that scenario into play.

According to the company, since we had not demonstrated any real prejudice to Canadians, we did not have the legal jurisdiction to speak out. I don't think the notion of *Safe Harbor* is an obstacle in this case.

You referred to the lack of awareness. It's quite possible that at a certain point in the evolution of this company, the executives were relatively naive and may indeed have lacked awareness to some degree.

However, my concrete experience leads me to think that this is not a matter of the lack of awareness. The executives say that they want to do better. The regulatory agency says to the executives' representatives that they must do better because according to that agency, they have broken the law. The executives are then aware of that fact, and yet they still decide not to act.

Mr. Michel Picard: In the documentary, Mr. Zuckerberg says, verbatim, that he will co-operate in order to comply with government requirements. But according to other former directors, he did not walk the talk.

Is the nature of the service provided by Facebook, if I compare it to a highway, simply that of a paved highway on which there is personal and commercial traffic, and advertising, and so on? There is free circulation on the highway, which the company has paved widely, so as to have as much traffic as possible.

Anyone who wants to watch the traffic on the highway can sit on the sidelines and watch it go by. The third party looks at what is going by on the platform, so that the very nature of Facebook's activities—in its eyes—frees it from any responsibility we would like to attribute to it.

I am trying to eliminate the arguments in its favour so that we may have all the necessary tools to consider even more coercive means than the ones we have at present.

● (1635)

Mr. Daniel Therrien: The analogy between Facebook's platform and a highway is not a bad one, but I would say that one of Facebook's positions is to say that it is a company that does business with consumers, on the one hand, but also with other companies, on the other hand, and it is these other companies that collect information from users.

Facebook says that it is not responsible for what the other companies do, and it asks to be held accountable only for its responsibilities, and not for the activities of other companies. That might hold, if not for the fact that Facebook has a commercial interest in having an enormous amount of traffic on its highway and in having other companies collect information.

It's not a sin for Facebook to make money, but the fact of developing business relationships from which it derives profits, and thus do business that is increased by the presence of third-party apps, is accompanied by legal obligations.

Mr. Michel Picard: The legal obligations apply because of the nature of the agreement with a third party and not as a consequence of the bad behaviour of the third party itself, correct?

Mr. Daniel Therrien: With regard to PIPEDA, it's one of the basic questions we are going to submit to Federal Court.

What's going on in our opinion is disclosure by Facebook to the third party. The user provides information to Facebook. Facebook has the information and communicates it to the other company.

The disclosure is an activity that is accompanied by legal consequences for Facebook. Facebook must see to it that the user provides informed consent for that activity.

We believe that this sets aside the argument according to which Facebook is not responsible for what its neighbours or business partners do.

Mr. Michel Picard: I have a hypothetical scenario which may not be very likely, but I will present it to you, nevertheless.

The Canadian Facebook market is about equivalent to the California market, if one takes population into account.

There are more than a billion Facebook users. I think that one person out of three in the world is on Facebook.

If we bother it too much, the company will simply leave Canada. Is that a consequence we can consider, and can we deal with it?

Are we now in a dead end that prevents us from acting to suit ourselves?

Mr. Daniel Therrien: I would approach the question in the following way.

Facebook is very successful because people want to communicate with their friends and family. It's a real need. Does that need have to be met by a company called Facebook, or would there be other companies that could provide social networks that could meet the needs of Canadians?

It would be more complicated. There would be fewer people on that social network, but I think that is how we have to look at it.

If a company, no matter how important it is, decides to leave because it does not want to comply with the law, I believe there will be other players that will take its place. There is a real need, and other players will want to meet it while complying with the law.

Mr. Michel Picard: Thank you.

[*English*]

The Chair: Next up for five minutes is Mr. McCauley.

Mr. Kelly McCauley (Edmonton West, CPC): Thank you, gentlemen, for your rather honest and sometimes disturbing testimony.

I'm a guest today on the committee, so I'll ask you to bear with me.

What recourse, in the absence of stronger legislation, do we have to deal with what you've stated, that Facebook has violated PIPEDA? Is there any?

Mr. Daniel Therrien: Legally, there is nothing in terms of privacy violations.

Mr. Kelly McCauley: My follow-up question to that is that I'm wondering how much of Facebook's actions are maybe due to a perceived weakness among our position. One of the things I find very disturbing in all of this—and this comes out of another committee I serve on—is government is moving all of our advertising out of local Canadian newspapers and radio and pushing a large share to Facebook. I have to wonder about the laughs they might be having in their head office knowing they're fighting with you over PIPEDA, but at the same time the government is pushing taxpayers' money to them.

Then I look through your departmental results and I look at how we, as a government, take privacy rather less seriously. I'm looking at a National Post report. When a National Post reporter asked a question of PSPC and DND, within an hour and a half they got a threatening phone call from the president of Irving, threatening a lawsuit because PSPC and DND gave away private information for the third time. The government gave away private information to a corporation.

I look at your departmental results and look at the percentage of government organizations that are informed and guided to protect privacy rights. Our target is only 60% of government organizations to actually follow our own rules. I wonder if Facebook looks at this and just thinks that if you guys aren't serious about privacy anyway, why should they be? Oh, and by the way, at the same time they'll take taxpayers' money from us.

I'm outraged, frankly, at the stupidity of it all. The same time that you're fighting against them, the government's handing them cheques, and at the same time—

● (1640)

Mr. Nathaniel Erskine-Smith: Billions of people use Facebook.

Mr. Kelly McCauley: Yes. Could I add another one?

Mr. Daniel Therrien: My answer would be this: A number of actors in society could take action to move away from companies that violate their privacy. The government has spending powers for advertising, but often the case is made that individuals also have a choice and could decide not to be on that platform. The fact remains that Facebook has two billion users and it's not easy for an individual to withdraw from that service. It's possible, but it's not obvious.

Mr. Kelly McCauley: We could switch back—

Mr. Daniel Therrien: This leads me to the solution. I do not think it is for individuals to have all of the responsibilities. Perhaps government could take some action by refusing to do business with a certain company that may have more impact, but that's not the true solution either. The true solution is to ensure that companies that meet a need in society—and clearly there's a need for people to communicate—do that in a way that respects the rights of Canadians. That means legislation.

Mr. Kelly McCauley: There seems to be a lack of outrage over it. There was a blip with Cambridge Analytica, which was very serious. Do you get the sense that, day to day, Canadians are just saying that it's a free service and if people don't want their privacy taken, don't use it? Is there just a lack of understanding of how serious this is or a lack of concern?

Mr. Daniel Therrien: I think people use these services because they have a need to function in a modern society. Modern society includes social media and relying on digital services. They would rather do that in a way that does not put their privacy at risk, but they feel they have to do that. Again, I think our task is to ensure that Canadians can have the benefits of the digital economy, but in a way that does not create harm for them, which brings me back to legislation.

Mr. Kelly McCauley: Thanks.

The Chair: Next up, we'll go to Ms. Vandenbeld for five minutes.

Ms. Anita Vandenbeld (Ottawa West—Nepean, Lib.): I think the previous question goes to the heart of the problem, which is the dilemma when you have these big data-opolies and choice is really not a real choice in terms of users or anybody else.

When you started this investigation, of course it was Cambridge Analytica and Facebook and the data breach. We, on the committee, have found that AggregateIQ was an integral part of that. Is that study still ongoing?

Mr. Daniel Therrien: It is, jointly with RBC colleagues, and we hope that later this spring we will be able to announce our conclusions.

Ms. Anita Vandenbeld: Without pre-empting the conclusions, is there anything you anticipate coming out of that study that would add to your recommendations on what this committee—

Mr. Daniel Therrien: —on legislation?

● (1645)

Ms. Anita Vandenbeld: Correct.

Mr. Daniel Therrien: It's difficult to say, and if I say, I may disclose the conclusions prematurely.

Ms. Anita Vandenbeld: We'll wait in great anticipation for the report.

Mr. Daniel Therrien: Okay.

Ms. Anita Vandenbeld: The concern I have, and you mentioned this a little bit earlier when you said that Facebook has millions of apps, is that Cambridge Analytica is just one app.

Mr. Daniel Therrien: Yes.

Ms. Anita Vandenbeld: We've been told in this committee that this is just the tip of the iceberg, and we know there are many other data platforms and social media platforms. Do you have concerns beyond Facebook of other data platforms? If so, given that you don't have the proactive ability to investigate, how would you recommend that we make sure we are able to investigate when these kinds of breaches may be happening in places that we are not even aware yet?

Mr. Daniel Therrien: Of course I'm concerned. Right now under the current law, we largely investigate based on complaints. We initiate a few complaints ourselves, but that's truly the tip of the iceberg.

Proactive inspection powers have to be seen in the following light. We will never, as a regulator, be able to monitor the activities of all companies. That's not the point, but if we have the authority to proactively inspect practices where we think there might be something untoward happening, and then find in some cases that something untoward is happening that carries consequential penalties, that sends a message to the whole industry that, if they violate the law, they are at risk of being inspected by the Office of the Privacy Commissioner and of incurring these fines.

With a system like that, there are much greater chances that behaviour across the sector will be improved.

Ms. Anita Vandenbeld: They are intricately intertwined, the ability to proactively investigate and be able to impose penalties.

Mr. Daniel Therrien: Yes.

Ms. Anita Vandenbeld: With regard to Facebook, the fact that they didn't implement the recommendations in 2009 and that they have rejected and not even acknowledged that there was wrongdoing in this case, do you believe that the kind of thing that happened with Cambridge Analytica, when people in Canada today are on Facebook, could still happen today?

Mr. Daniel Therrien: There is no question that it could happen today.

Ms. Anita Vandenbeld: That's not just on Facebook but on other platforms as well.

Mr. Daniel Therrien: It could. I haven't investigated others, but I assume that what is happening on Facebook may be occurring elsewhere, but certainly with Facebook, yes.

Ms. Anita Vandenbeld: I would imagine that there is a lot of urgency in terms of our need to be able to legislate so that you can have those kinds of powers.

Mr. Daniel Therrien: Yes.

Ms. Anita Vandenbeld: Going to the Federal Court obviously would allow penalties, but your estimate is that would be another year. It would add a lot of time, and then we wouldn't be able to have that kind of urgency in terms of your investigations. Is that correct?

Mr. Daniel Therrien: It would take a year. After a judgment by the Federal Court, I think we would be in a much better position, but I'm not sure that the legal proceedings would stop at the Federal Court. I think what is at play is sufficiently near to the business model of the company that it is likely this matter would reach the appellate court level, so it's going to take some time.

Ms. Anita Vandenbeld: Thank you.

The Chair: Next up for five minutes we have Mr. Gourde.

[*Translation*]

Mr. Jacques Gourde: I found your last statement interesting. We certainly won't get to the Court of Appeal overnight. We're looking at a 10-, 15- or 20-year horizon.

Mr. Daniel Therrien: Five years.

Mr. Jacques Gourde: That's rather optimistic.

Canada is really the Far West when it comes to the digital landscape and its regulation. We want to do something, but what? Are there countries that have chosen collective action or more or less common legislation with other countries, which could send a signal to Facebook and to other large companies to incite them to develop a framework?

Canada can try something. It may be sued. There may be winners and losers. Other countries will be watching. Do you think every country will adopt measures, individually, at the same time? Will the laws ultimately be similar?

Mr. Daniel Therrien: I don't think we will see an international treaty any time soon, either.

If different countries adopt similar or interoperable laws, the multiplication of those legislative and regulatory measures could lead to results. What's encouraging, as you know, is that Europe has already passed regulation that provides some solid privacy protection. It came into effect about a year ago.

I'm encouraged by the fact that serious discussions are now being held by the American Congress to adopt privacy protection legislation. When our trading partners in Europe, the South and several Asian countries go in the same direction, there is reason for greater optimism but it's taking a long time.

Ultimately, the adoption of stricter laws in various countries, some of which are Canada's trading partners, should improve things.

● (1650)

Mr. Jacques Gourde: I believe that Canadian legislation would be more restrictive with regard to Facebook than American legislation. In the American system, Facebook must give a lot of money to members of Congress. There must be pressure to ensure a certain amount of leeway and freedom in reality. However, the political systems of countries such as the United Kingdom, Canada and Australia may provide an opportunity to take things a little further.

You've adopted a strategy of taking small steps, and that's fine for you. However, should we, the legislators, work with four or five countries to test the system properly? Otherwise, one country will act, and other countries will observe what happens and then make adjustments one after the other. Is the best approach to wait for one country to act and then make adjustments as the initiatives unfold, or to ensure that the countries take stronger measures? The latter approach would send the message that recess is over.

Mr. Daniel Therrien: All countries must act, without waiting to see what their neighbours will do. We're back to the initial point of the conversation, which is that technology and business models are evolving very quickly. We shouldn't think that if the legislation is amended in two years, it will be effective for the next 20 years. The legislation must be effective when it's passed and flexible enough to take into account technological changes. Parliamentarians must also keep an eye out for these changes and must act quickly when the legislative framework shows weaknesses in this area.

In today's world, technology is changing at an incredible rate. The legislation isn't keeping up, and that's a major issue. I'm not asking for the legislation to be amended every six months. However, we must establish a framework that's flexible enough to take into account technological changes, while keeping in mind that it may be necessary to legislate five or eight years down the road because of the speed of these changes.

Mr. Jacques Gourde: Our legislation must be very progressive and proactive.

Mr. Daniel Therrien: Yes, exactly.

Mr. Jacques Gourde: Do you want the government to make it a priority in the future?

Mr. Daniel Therrien: Absolutely.

Mr. Jacques Gourde: If the legislation isn't a priority, it may be postponed. However, if the legislation is a priority, things may move faster.

Mr. Daniel Therrien: What could be a more serious consequence for a society than business practices that undermine the integrity of the democratic process? This is the first of several reasons to take urgent action. The new Parliament should make it a priority to legislate on these issues.

Mr. Jacques Gourde: Thank you.

[*English*]

The Chair: Go ahead, Ms. Fortier, for five minutes.

[*Translation*]

Mrs. Mona Fortier (Ottawa—Vanier, Lib.): Thank you, Mr. Chair.

Thank you for joining us, Mr. Therrien.

The questions are starting to become repetitive, and I hope that I won't make you repeat yourself.

We're obviously discussing a complex matter. We must find a way to monitor developments on this issue.

You've already answered a number of my questions. In your presentation, you said that it was time to reform the legislation. I think that's clear. You said that the legislation should require demonstrable responsibility, which would be similar to accountability. You've probably done so, but could you briefly explain what you meant by that?

● (1655)

Mr. Daniel Therrien: Yes.

In the current legislation, the first principle is referred to as "accountability" in English and "*responsabilité*" in French. As I understand it, the term "accountability," in an accounting sense, means a "*reddition de comptes*." In other words, it means that the responsible party must report to its constituents on how it has carried out its responsibilities.

In the current PIPEDA, the term "accountability" is referred to as "responsabilité" in French. Responsibility ends before accountability. It's already a lot, but it ends before accountability. Responsibility consists of adopting procedures to implement the other principles of the legislation, including consent, openness and access.

The company or organization fulfills its obligation to take responsibility by adopting procedures. However, the company or organization isn't accountable, either to users or to the regulatory agency, when it comes to demonstrating that the procedures implement the PIPEDA principles.

One consequence of Facebook—and there are other signs of this—is that it can no longer be trusted. The principle of accountability is important. Companies must take responsibility, and the entire privacy burden mustn't be placed on users. It would be unrealistic to think so. Companies must take responsibility.

The case of Facebook, for example, clearly shows that the fact that the legislation imposes a responsibility doesn't mean that the obligation will be fulfilled, hence the need to require accountability. Companies must be required to show that they've adopted procedures to implement the principles of the legislation, while providing proactive inspection powers.

Under one model, companies would provide a report to the regulatory agency on the procedures that they've adopted. The reports would be similar to the privacy breach reports, which have been a legal obligation since November.

Imagine legislation where companies must provide a report to the regulatory agency on the procedures that they've implemented to fully comply with the PIPEDA principles. The regulatory agency, which has limited resources, would review the reports and note issues in certain places. It would inspect the companies, and perhaps it would find violations and penalize the companies.

If responsibility were to lead to true accountability,

[*English*]

a real accountability in accounting terms,

[*Translation*]

it would eventually have an impact on the entire industry, because companies wouldn't want to run the risk of being inspected and penalized.

Mrs. Mona Fortier: Thank you.

I have one last question. Is there anything that we haven't yet addressed in this committee and that we should look at before the end of this Parliament and afterward?

Mr. Daniel Therrien: Responsibility is a key issue. You may have heard industry representatives say that, in the modern technological world, consent isn't always realistic and that companies can step in and take responsibility for how they handle information.

Again, I don't see any issue with companies taking on some of the responsibility. However, we must seriously consider the fact that it isn't enough to make companies take responsibility. An audit must be carried out by an independent agency, which acts on behalf of individuals, who are often unable to identify the issues. Companies know their business model and are generally responsible. However, a third party must ensure that the interests and rights of users are actually upheld.

● (1700)

Mrs. Mona Fortier: Thank you.

[*English*]

The Chair: Mr. Angus.

Mr. Charlie Angus: Thank you, Mr. Chair.

I want to follow-up on your comments about accountability, because I'm trying to think of a similar situation where there is a corporate lack of accountability. Facebook has an enormously successful platform. It's used all over the world. It's making unprecedented money. It has no competition and yet, in this past year, the U.K. parliamentary committee has made a finding that it was a digital gangster and the privacy commissioner in New Zealand found it to be morally bankrupt. Facebook was denounced by the UN for complicity in the Myanmar genocide.

It would seem to me that normal corporate practice would be to get on a goodwill tour and start to fix the problems and reassure people, yet Mr. Zuckerberg ignored his appearance at the International Grand Committee, and now we have your report coming out.

Facebook said, "Thanks, but we don't want to spend any money to actually comply, so we'll just pretend you don't have jurisdiction over law." You referred to its policy as an empty shell. I'm trying to figure out what is fundamentally wrong with Facebook.

Is it the corporate culture, which I'm not asking you to venture in on, or is it that its fundamental business model, like the fundamental business model of surveillance capitalism, is based on ignoring the privacy rights of citizens, and it simply will not change a business model that has worked extremely well for it, even if it is breaking the law of Canada and numerous other jurisdictions?

Mr. Daniel Therrien: It's clear that its business model, like the business model of many companies, is to monetize the value of personal information. That's the core of the issue and we need, as societies, to develop the right legal framework to ensure that whatever service actually adds value is maintained, but in a way that does not create harm, because of the collection and ultimately, corporate surveillance of citizens.

Mr. Charlie Angus: Finally, in order to prevent something like this in the future, so that when a Canadian regulator steps in and starts to investigate, because there will be other breaches—there could be other even more serious breaches—what tools are you asking for? You need to repeat it to our committee, so we can repeat it to the Parliament of Canada. W need to learn from the lessons of the Cambridge Analytica scandal, so we can protect the democratic and social rights of citizens who use online services.

Mr. Daniel Therrien: My recommendations are to give stronger enforcement powers to my office as the regulator, which means in practice at least three things: the authority to make binding orders; the authority to impose penalties to make sure that these orders are actually implemented; and equally important, perhaps more important, the authority to proactively inspect the practices of companies to make sure that they actually follow the law. That's an important mechanical step.

Beyond that, we need to reform the principles of the private sector law and the public sector law, but now we're talking about the private sector law. I don't have a problem with the fact that the current PIPEDA is principles-based. It's part of the architecture that allows it to endure over time, regardless of technologies. But this principles-based legislation also needs to ensure that it is rights-based and defines privacy not as a series of important mechanical steps like consent, but defines the right at the proper level, which is the right to be free from unjustified surveillance by corporations and government. That's the right that's at play, and that's the right that needs to be enacted, I believe, so that citizens can engage in the digital economy, can make searches and can develop as persons in such a way that they can do that without being subject to constant surveillance.

● (1705)

The Chair: Thank you, Commissioner Therrien.

Once again, it's never long enough, but we appreciate your appearing at our committee.

We have committee business right away, so I'd ask you to keep the exit as brief as possible.

[*Proceedings continue in camera*]

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

SPEAKER'S PERMISSION

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

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

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

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

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

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

PERMISSION DU PRÉSIDENT

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

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

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

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

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