HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 100 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, April 19, 2018

Chair

Mr. Bob Zimmer

Standing Committee on Access to Information, Privacy and Ethics

Thursday, April 19, 2018

● (0850)

[*English*]

The Chair (Mr. Bob Zimmer (Prince George—Peace River—Northern Rockies, CPC)): Thank you, everybody, for coming today to meeting number 100 of the Standing Committee on Access to Information, Privacy and Ethics. Pursuant to Standing Order 108 (3)(h)(vii), we are studying the breach of personal information involving Cambridge Analytica and Facebook.

With us today are Kevin Chan, global director and head of public policy, Facebook Canada, and, via teleconference from California, Robert Sherman, deputy chief privacy officer.

I would like to start with Mr. Chan. We, and I as chair, were disappointed that Mr. Zuckerberg declined our request. We don't take that lightly, but we appreciate your being here today.

Mr. Chan.

Mr. Kevin Chan (Global Directeur and Head of Public Policy, Facebook Canada, Facebook Inc.): Thank you very much.

Again, yes, our CEO does apologize that he could not be here today in person with the committee. I am here with my colleague Rob Sherman on his behalf. Thank you for that note, sir.

Mr. Chair and members of the Standing Committee on Access to Information, Privacy and Ethics, thank you for the invitation to appear before you today. My name is Kevin Chan, and I am the head of public policy for Facebook Canada. I am joined via video conference by my colleague Rob Sherman, Facebook's deputy chief privacy officer.

Before I start, I want to acknowledge our offer earlier this week to pre-brief committee members on the Cambridge Analytica situation. Over the past few weeks, we have made a large volume of announcements for which we have done pre-briefs to U.S. lawmakers prior to last week's congressional hearings. We want to extend that same offer as a courtesy to members of this committee. I regret that our intentions may have been unclear.

I want to begin by sharing that while we do not yet have all the facts surrounding the situation with Cambridge Analytica, what has alleged to have occurred is a huge breach of trust to our users, and for that we are very sorry.

Given the scale of our service, with more than 23 million Canadians using Facebook every month—and more than 2 billion people globally—we recognize the role we play in people's lives and the need to take greater responsibility for that.

[*Translation*]

It goes without saying that the events of recent weeks involving the protection of personal data is of concern to us all. With hindsight, it is clear that Facebook had not invested enough in the security of our platform, and, for that, we are responsible. We have a duty of extreme vigilance and we are going to do everything we can to make the required corrections in order to regain the trust of those who use the platform.

[*English*]

The events of the last few weeks have taught us some important lessons. Trust in our service is at the core of what we do at Facebook. As our CEO Mark Zuckerberg recently said, “We have a responsibility to protect your data, and if we can't then we don't deserve to serve you.”

As Facebook has grown, people have gotten powerful tools to stay connected to those they care about, make their voices heard, and build communities and businesses, but it's clear now that we didn't do enough to prevent these tools from being used for harm as well. We didn't take a broad enough view of our responsibility, and that was a mistake.

In Canada and around the world, we know we have a lot of work to do, and this is just the beginning. We are of course also fully co-operating with the Office of the Privacy Commissioner of Canada as it conducts its investigation into the matter.

I would like to turn now to my colleague Rob Sherman, who can take you through some of the facts as we know them today and the actions we are taking to prevent abuse from happening on our platform going forward.

Mr. Robert Sherman (Deputy Chief Privacy Officer, Facebook Inc.): Thank you, Kevin.

Thank you to the committee for having me here today.

As Kevin mentioned, I'm Facebook's deputy chief privacy officer. I want to apologize for not being able to join today's committee hearing in person. I'm hosting a summit today in California with many leading privacy experts, a summit that had been scheduled for some time. I appreciate the committee's attention to this important matter, and we appreciate the opportunity to provide information to support your study.

I'd like to spend just a few minutes on the specifics of this situation and what we're planning to do going forward.

In 2015 we learned from a report in *The Guardian* that a Cambridge University researcher named Aleksandr Kogan had shared data from a quiz app that he operated on the Facebook platform, This Is Your Digital Life, with Cambridge Analytica. It is against our policies for developers to share data without people's consent, so we immediately banned Dr. Kogan's app from our platform and demanded that Dr. Kogan and certain other entities he had relationships with, including Cambridge Analytica, delete any information they had received.

Several weeks ago we saw press reports alleging that some of this information may not have been deleted as Dr. Kogan, Cambridge Analytica, and others had certified. Based on our own data, we estimated a total of 305,000 people around the world had installed the app This Is Your Digital Life and that an additional 86.3 million were friends of people who had installed that app and were therefore potentially affected by data sharing.

While the vast majority of these people were in the United States, we estimate that 272 people in Canada installed the app, potentially affecting 621,889 additional Canadians. This represents 0.7% of the people affected across the world.

We take each case with the utmost seriousness, and that is why we're informing people if there is even a possibility that they may have been affected.

We have a responsibility to make sure that what happened with Cambridge Analytica does not happen again, so we've undertaken a series of steps to increase the protections we're providing for people's information. Here are some of the steps.

First, we need to make sure that developers like Dr. Kogan who got access to a lot of information in the past cannot get access to as much information anymore. We already made changes to the Facebook platform in 2014 to dramatically restrict the amount of data that app developers can receive and to proactively review apps before they can use our platform. Because of these 2014 changes, a developer today would not have access to the same amount of data that Dr. Kogan was able to obtain.

However, there is more that we intend to do to limit the information developers can access and to put more safeguards in place to prevent abuse. For instance, we're removing developers' access to your data if you haven't used their app in three months. We're reducing the data you give an app, when you use the new version of Facebook login, to only your name, your profile photo, and your email address. That's a lot less than is available to developers on any other major app platform. If a developer wants to use Facebook login to obtain more information than this—for example, access people's posts or other private data—we'll require them to sign a separate contract with us that imposes strict requirements.

Second, we're in the process of investigating every app that had access to a large amount of data before we locked down our platform in 2014. If we detect suspicious activity, we'll do a full forensic audit. If we find that someone is improperly using data, we'll ban them and we'll tell everyone affected.

Finally, we're making it easier to understand to which apps you've allowed access to your data. This past week we started showing everyone a list of the apps they've used and then an easy way to revoke permissions they've granted to those apps in the past. This is something you can already do in your privacy settings, but we're putting it at the top of the news feed to be sure everyone sees it.

We've also announced proposed updates to our data policy and terms of service to provide more information about our data practices and the choices people have. We hope this will better enable people to make informed decisions about their privacy and to better understand how we use data across Facebook, Instagram, Messenger, and our other services.

I'd now like to turn it back to my colleague Kevin to talk a bit about what we are doing with respect to election integrity in Canada.

● (0855)

Mr. Kevin Chan: Thanks, Rob.

[*Translation*]

We recognize that the situation involving Cambridge Analytica raises more general questions on the use of Facebook and the integrity of elections. I would like to conclude with some comments on the subject, because we are working hard to do our part to protect the integrity of the federal elections in 2019. We know that your leaders and your political parties continue to use Facebook as a key platform for citizen involvement. So it is important that the matter be taken seriously.

[*English*]

As you may know, the Communications Security Establishment published last year a report outlining various cyber-threats to the next federal election and identified two areas Facebook sees a role in addressing: cybersecurity, the hacking into the online accounts of candidates and political parties; and the spreading of misinformation online. In response, we launched, last fall, our Canadian election integrity initiative, which consists of five elements.

First, to address cybersecurity, we launched the Facebook “Cyber Hygiene Guide”, created specifically for Canadian politicians and political parties. It provides key information on how everyone who is administering a political figure or party's Facebook presence can help keep their accounts and pages secure. I have brought copies of the guide with me, Mr. Chair, and with your permission, later I will circulate them to members.

Second, we are offering cyber-hygiene training to all the federal political parties.

Third, we launched our cyber-threats email line for federal politicians and political parties. This email line is a direct pipe into our security team at Facebook and will help fast-track responses for compromised pages or accounts.

To address misinformation online, we've partnered with MediaSmarts, Canada's Centre for Digital and Media Literacy, on a two-year project to develop thinking, resources, and public service announcements on how to spot misinformation online. This new initiative, which we are calling “Reality Check”, will include lesson plans, interactive online missions, videos, and guides that will provide the idea that verifying information is an essential life and citizenship skill.

We also launched our ads transparency test, called “View Ads”, here in Canada last November. This test, which is ongoing, allows anyone in Canada to view any and all Facebook ads, including ads for which you were not the intended audience. All advertisers on Facebook are subject to “View Ads”, but we recognize that it is an important part of our civic engagement efforts. Candidates running for office and organizations engaged in political advertising should be held accountable for what they say to citizens, and this feature gives people the chance to see all the things a candidate or organization is saying to everyone. This is a higher level of ad transparency than currently exists for any type of advertising, online or offline.

[*Translation*]

As we answer your questions, Rob and I hope that we can tell you more about our efforts to protect personal information and the integrity of elections. We recognize that, in the past, we have been too idealistic about the use of our technologies and we have not concentrated sufficiently on preventing abuse on our platform. We are in the process of making major changes in the operation of our company in order to improve our approach in that regard.

[*English*]

Thank you again for the opportunity to appear before you today, and we would now be pleased to answer your questions.

The Chair: Thank you, Mr. Chan and Mr. Sherman.

First up, for seven minutes, is Mr. Erskine-Smith.

● (0900)

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

First, have you notified Canadian users, and if so, exactly how have you notified them?

Mr. Robert Sherman: Thank you very much for the question.

We're in the process of notifying people in Canada and globally about the situation. The way we will let them know is through information at the top of their news feeds that will explain that they have access to information about which apps have received their information. If they are affected by Cambridge Analytica, they will be notified about that as well.

Mr. Nathaniel Erskine-Smith: If people have deleted their Facebook accounts, they wouldn't have any ability to be notified, in all likelihood.

If a company cared more about users than its share price, and it learned about a breach in 2016, wouldn't it have notified its users in 2016?

Mr. Robert Sherman: I think it's important to note that the trust of people who use Facebook is paramount, and it's critical not only for our ethical obligations but for our business obligations as well, because we realize that if people don't feel that their information is protected on Facebook, they won't feel comfortable using our services. So while certainly information about—

Mr. Nathaniel Erskine-Smith: So why didn't you notify users in 2016?

Mr. Robert Sherman: I think what our CEO Mark Zuckerberg has said is that in retrospect is that we should have done that. Going forward, if a situation like this occurs, then we will certainly do that.

Mr. Nathaniel Erskine-Smith: In the international context, 350,000 or so people consented to using an application and allowed the ap developer to access 87 million user profiles. In Canada, if I have it right, 272 people accessed it, giving access to 620,000-plus Canadian user profiles. How is that in compliance with the existing law?

Mr. Robert Sherman: I think those numbers are generally correct, but it's important to note that we have taken a conservative approach here. We don't have perfect information about exactly which information was transferred at which time. What we have aimed to do is err on the side of caution and notify more people rather than fewer people.

Mr. Nathaniel Erskine-Smith: I appreciate that in terms of the numbers, but in terms of our legislation here in Canada, PIPEDA, which requires consent—usually explicit consent, and in some cases implied consent—where was the consent of 620,000 users?

Mr. Robert Sherman: The approach we took at the time...and as I mentioned in my opening statement, we've made significant changes to the platform since this information was available to restrict the information that app developers can receive.

For the 272 people who specifically authorized the app, there was a screen that popped up that would have notified them of what information the developer wanted to receive, and they would have clicked it to accept—

Mr. Nathaniel Erskine-Smith: They can't consent on behalf of other people, right?

Mr. Robert Sherman: With regard to the—

Mr. Nathaniel Erskine-Smith: Sorry. You've made changes, and perhaps you're in compliance with the law now, but it seems pretty clear that you weren't in compliance with the law previously. Is that fair?

Mr. Robert Sherman: With regard to the people who are friends of those who were using the app, our data policy and our disclosures at the time were very clear that this was how the platform worked. It's important to note that as our changes in 2014 reflect, we don't think that's the right way for a platform to operate, and it's not the way the platform operates today.

This is something that at the time and since, we've been in discussions with the Privacy Commissioner of Canada about. So while we think it's not the appropriate way for a platform to operate, we also want to make sure we're in compliance with all applicable laws.

Mr. Nathaniel Erskine-Smith: Not only is it not an appropriate way, but the way you previously designed the system is also contrary to our law.

Mr. Zuckerberg has noted that you're open to regulation. You've taken some additional steps. What regulations specifically do you think would fix the problems that you've experienced?

Mr. Robert Sherman: There are a number of different steps that need to be taken, and the first one, as you pointed out, is that Facebook needs to take responsibility. We hope that we have, and we need to continue to do work to make sure that people's information is safe on our platform. That's something we've invested in and that we have a responsibility to do, over and above the law. As Kevin mentioned in his opening comments, we have a responsibility to take a broader view of what we should do.

From my conversations about privacy regulation in Canada and around the world, I think taking a principles-based approach that provides strong privacy protections to Canadians and to people everywhere is important. That's something that exists in PIPEDA today.

I know this committee is undertaking a study and has published a report with recommendations regarding PIPEDA, and there's a lot in that study that's worth considering, but I think PIPEDA's fundamental principles-based approach and giving the Privacy Commissioner broad authority and discretion in how to apply that to new technologies and new situations is an appropriate model.

● (0905)

Mr. Nathaniel Erskine-Smith: Though, interestingly, we had a principles-based approach previously, when Facebook disrespected those principles and failed to abide by our existing legislation.

In 2014 you made changes, but all of those app developers who have previously collected information still have that information. Can you give a sense to Canadians of exactly what detailed information that entails?

My understanding is that app developers would have had access to the education, work affiliation, personal relationships, friend lists, likes, location. What else?

Mr. Robert Sherman: Obviously, the specific information that's affected depends on the specific app.

Mr. Nathaniel Erskine-Smith: What's the worst situation, the most personal information that would have been shared with app developers?

Mr. Robert Sherman: App developers would have been able to receive information that people have shared on their profiles—things such as their likes, their city, where they live, and that kind of information.

We've made changes since then, and those were pieces of information that were shared under the privacy settings of the person affected. You would have had the ability to choose whether to share the information in the first place. You would have had the ability to choose who to share it with, so you might have shared it with some friends but not others. And you would have had the ability to choose whether those friends could bring that information to apps.

As I mentioned, since then we've significantly restricted the amount of information that's available to apps.

Mr. Nathaniel Erskine-Smith: There's an app developer of a game called Cow Clicker who posted about it on *The Atlantic*'s site. He said it was a really rudimentary game. If I had clicked on that app and played this ridiculous Cow Clicker game, the developer would have had access to my friends' marital statuses. Does that make sense to you?

Mr. Robert Sherman: It doesn't. It's one of the things in our developer policies, which we require all developers to abide by. We impose a series of restrictions on what information they can collect and how they can use it. Among those restrictions is a rule that says developers cannot ask for more information than they need to operate the service they're providing. Since 2014, we've operated an upfront review process that looks at that, among many other things. But certainly, it's not our intention that apps use the Facebook platform to collect information they don't need. As we announced several weeks ago, we're making much more significant restrictions in the amount of information that most apps can get.

Mr. Nathaniel Erskine-Smith: Unfortunately, those changes are only being made now that this situation has been made public and not because you ever thought it was the right thing to do.

Thanks very much.

The Chair: Thank you, Mr. Erskine-Smith.

Next up, for seven minutes is Mr. Kent.

Hon. Peter Kent (Thornhill, CPC): Thank you, Mr. Chair.

Thank you, Mr. Chan and Mr. Sherman, for attending this committee today. It's good to see you again.

These data mining scandals seem to have finally penetrated the consciousness here in Canada that the data world is one that is largely without national boundaries, without effective protection or regulation of the personal information that Canadians voluntarily or unconsciously surrender as their part of the contract to use your service. In many ways, it is a fine service; I use it politically and have no complaints in that area. But, of course, our focus here is on the abuses that data mining has, and would potentially have, to interfere in our democratic process.

Where should Canadians look at Facebook for responsibility and accountability: to your Canadian entity or to the parent company? When did Facebook Canada learn of the abuse of personal users' privacy, and did Facebook Canada, Mr. Chan, individually and separately, hold back the reporting of that abuse for two years as the parent company did? Were you aware of that breach for the past two years?

Mr. Kevin Chan: No, sir. To talk about the particular instance, we knew, I think, as everybody learned through press reports—I forget the exact date—about a month ago or something like that, sir. That would be the extent of our knowledge in Canada.

Hon. Peter Kent: As you know, our Conservative government strengthened Canada's Personal Information Protection and Electronic Documents Act, PIPEDA, just before the election in 2015. This Liberal government, after sitting for three years on creating some of the regulations introduced in that legislation for the breach of security safeguards regulations, yesterday very quietly posted regulations on the *Canada Gazette* regarding the timely reporting of breaches to the Privacy Commissioner and to affected individuals.

Can Facebook Canada assure this committee that at the next violation of users' privacy, Facebook won't hold back that information for two years as it did in this case?

● (0910)

Mr. Kevin Chan: Sir, absolutely, we are already taking action, as Rob mentioned. We are already taking action to notify all users of the particular instance regarding Cambridge Analytica. Our commitment, and the commitment of our CEO, is that, in fact, we're going to go back and do an audit of all the other apps that were in place at the time when the platform permissions were set a certain way. If we find evidence of wrongdoing there, we will also suspend and prevent those apps from functioning on Facebook. Then we will notify all potentially affected users for those apps as well.

Absolutely, going forward, that is very much our intent, sir.

Hon. Peter Kent: Thank you.

When elements of our committee visited Facebook's headquarters in Washington last October—and thank you for your hospitality, for sharing assurances on the company's commitment to social media operations and precautions, and for the demonstrations of some of the wonderful new products, like the oculus virtual reality devices—we discussed in general the possibility of new regulations here in Canada with regard to PIPEDA, or perhaps even going beyond the existing regulations with more meaningful regulations and penalties for violations of Canadian users' privacy.

We were told, almost in passing, that any new Canadian regulations might well put at risk Facebook investments in Canada along the line of the $7 million invested in the artificial intelligence project in the Montreal hub.

I wonder whether today, after Cambridge Analytica, AIQ, and Mr. Zuckerberg's testimony in Washington last week, that same caution against more meaningful regulation would still be made by Facebook to Canada?

Mr. Kevin Chan: Sir, I will turn to Rob for the more specific answer about what the prospective view is. I just want to be very clear, sir, that we certainly do not base our investment decisions on the specific regulatory environment. In particular, I did read some reference to some interview somewhere about about our AI research centre specifically. I just want to be very clear that it is not at all our view. That is not the representation we would have made. In fact, it's quite the opposite: we are quite proud to be supporters of AI in Canada, in Montreal and in Quebec. We are a global leader in this regard and Facebook is very proud to be part of that. I just want to be very clear.

Just last week we were in Montreal where we held an event in partnership with the Canadian Institute for Advanced Research celebrating the Montreal AI ecosystem. At no time would we have made investment in our AI lab contingent on any other consideration than the fact that there is talent in Canada and we feel fortunate and honoured to be a part of that.

Hon. Peter Kent: Mr. Sherman.

Mr. Robert Sherman: Sir, with regard to the PIPEDA study more broadly, we appreciated the committee's attention to this issue. Canadians deserve strong privacy protections and we appreciated the opportunity to provide information as part of that study.

I think in looking at privacy regulation more broadly, it's important, as the committee's report pointed out, that Canadians have information and transparency about how their information will be used and that they're in control of that information. A lot of those concepts exist in PIPEDA as it stands today. If you look at Facebook's history in Canada and our engagements with the Privacy Commissioner, a lot of the improvements, including many of the improvements that we talked about around the Facebook platform, come directly out of our engagement with the Privacy Commissioner.

I note that the committee has suggested several changes and improvements that might be made. I think it's appropriate to look at those, and one of the ones that you've already mentioned around data breach notification particularly is something that we've learned some hard lessons about and is certainly worth taking a look at.

● (0915)

Hon. Peter Kent: Just very briefly, one of our recommendations was for the government to consider more closely aligning with the European Union's general data protection regulation that comes into effect in May of this year. Would Facebook be comfortable, the parent company of Facebook Canada be comfortable, if Canada were to adopt similar GDPR regulations?

Mr. Robert Sherman: We think everybody who uses Facebook's service globally deserves strong privacy protections. That includes people in Canada, of course, and people in Europe. We've put in a lot of work, as we have in Canada, to provide those strong protections. As a part of our work to prepare for GDPR, we've built a number of new privacy controls settings and other engagements, and those are things that we plan to roll out in Canada as well.

Hon. Peter Kent: Thank you.

The Chair: Thank you, Mr. Kent.

Next up for seven minutes is Mr. Angus.

Mr. Charlie Angus (Timmins—James Bay, NDP): Thank you, Mr. Chan, Mr. Sherman, for joining us this morning. At the outset I want to say that Facebook in my region has been revolutionary. I represent a region that's bigger than the United Kingdom. I have communities that have no access to roads. I have some of the poorest communities in North America. The access that Facebook provides young indigenous people, for people contacting my office.... I don't use the phone anymore. If I have a medical crisis in Kashechewan, I get a message on Facebook and they get a response. So the power of Facebook to do good is incredible, but we are here because the power for Facebook to be misused for terrible things is also at issue.

The question before us is the failure of Facebook to respect the absolute power it has. The sense is that in some ways it thinks domestic laws are somehow quaint. I was very surprised this morning to learn that Facebook has shifted 1.5 billion users from Facebook Ireland to Facebook California to escape the GDPR.

Mr. Chan, will you tell this committee that as an act of good faith you will immediately implement the GDPR for all users in Canada for Facebook?

Mr. Kevin Chan: I think I'll let Rob address that one.

Mr. Charlie Angus: Mr. Chan, you represent Facebook Canada. He represents Facebook California. I want to know will you put in the GDPR? Will you commit today so that you don't have to be regulated to do it, but that Facebook will self-regulate in Canada with the GDPR. Yes or no?

Mr. Kevin Chan: Sir, I'm not aware of the point that you just raised. I'm not familiar with the point you say you've just learned.

Mr. Charlie Angus: We're talking about 1.5 billion users who were shifted to escape European law this morning.

Mr. Robert Sherman: Mr. Angus—

Mr. Charlie Angus: Will you just say, “We'll implement in Canada”? Then we can move on to the next question.

Mr. Robert Sherman: Mr. Angus, our plan is to provide the same privacy controls and settings that we're offering in GDPR, the same engagements on the same topics to people in Canada that we're offering to—

Mr. Charlie Angus: Will you implement the full GDPR? I mean, you tell us you're going to do tweaks. Why would you need to move 1.5 billion users out of the range of the European law?

Mr. Robert Sherman: I want to be clear. Prior to today, prior to our data policy changes, Canadians were served by Facebook Inc. in California, and the entity with which they contract was Facebook Inc. That remains the same, so there's no change with regard to Canadians.

Mr. Charlie Angus: We're here because of a social app that Aleksandr Kogan used that gave him access to 85 million users, which was transferred to a political entity that may have undermined elections around the world, and when Facebook became aware of this, Facebook claimed that this was absolutely not a breach.

How can you be trusted with self-regulation if, in the face of such a massive misuse of data, Facebook did not tell anybody because it thought it wasn't worth telling them because it wasn't a breach?

Mr. Robert Sherman: I think it's critically important that we uphold the trust of our community, and part of what we've learned as a part of this is that we need to communicate more robustly about what's going on in—

Mr. Charlie Angus: You say “communicate more robustly”. You became aware of this in 2015. You started telling Canadian users three weeks ago. That's not robust; that's your getting caught.

Again, the question before our committee is whether Facebook needs regulation because you cannot be trusted to do the right thing with personal information.

I want to reference Sandy Parakilas to you, who was brought in to fix the privacy problems at Facebook. He warned Facebook about numerous third-party apps, including a developer who was generating profiles of children without consent. He said that Facebook's response to him was that it did not want any negative press and that it wanted to deal with these issues to get them out of the way as quickly as possible. He proposed a deeper audit on how the data was being misused, and Facebook said, “Do you really want to see what you'll find?”

So I put it to you, Mr. Sherman, that obviously Facebook hasn't taken this issue seriously. We will have to look at regulation. Mr. Zuckerberg referred to regulation. Do you think Facebook has failed to represent the best interests of the people around the world who trust it?

● (0920)

Mr. Robert Sherman: I think it's certainly our intention to do the best we can in protecting the privacy and the information of users on our service. It's clear in this situation that we did not do enough. We're sorry for that, and we need to invest in doing more work.

With regard to notifying people about situations like this and notifying regulators, I think we found out about this in the first instance from news reporting. There was news reporting in the intervening period about this situation, and so it certainly was not something we intended to keep a secret. That said, I think notifying Canadians and others who are affected is something we should have done, and that we will do going forward.

With regard to the broader characterization of the discussions at Facebook, I don't remember working with Mr. Parakilas. He was at Facebook some time ago, and I'm not familiar with the specific discussion you're talking about—

Mr. Charlie Angus: My concern is the issue of a corporate culture that has so much power over data but seems so loosey-goosey about its use, and we're talking about data that may have undermined the integrity of international elections. Mr. Parakilas was brought in to deal with the privacy concerns of Facebook, and he said that the overriding issue time and time again was to get the negative stories to stop. So three weeks ago, in the middle of an international investigation, Facebook suddenly announced it was taking the privacy concerns of Canadians seriously.

Are you here, Mr. Chan, to engage with us on the issue of regulation, or are you just here to try to make the bad story stop, which seems to be Facebook policy, as Mr. Parakilas said?

Mr. Kevin Chan: Absolutely, sir, we are here to engage with you substantively. On the issue of regulation, I think our CEO, Mark Zuckerberg, has been very clear that we do not oppose regulation. I think we want the right kind of regulation, and I think—

Mr. Charlie Angus: Is GDPR the right kind of regulation for Canada?

Mr. Kevin Chan: If I may sir—

Mr. Charlie Angus: That's the question.

Mr. Kevin Chan: There are some other things that I wish to add with respect to regulation. I think maybe Rob would have some views on the specific question that you have with respect to privacy regulation.

I just want to point out to the committee, so that people have this in mind, that I think for a lot of the things, including election integrity, which you touched on, Mr. Angus, we are not waiting for regulation. In many respects on that front, we are not waiting for regulation. We think to be proactive and do things now, when we can, is the responsible thing to do.

I'd like to comment on two other things. The first is with regard to "View Ads", our ad transparency test in Canada. As you know members, obviously, there is no obligation to do that. We are actually rolling this out. We tested it first in Canada. Until this week, it was the only jurisdiction anywhere in the world where that was in place. Again, we are being proactive. We're not waiting for regulation. We're doing the right thing, based on what we learned coming out of the U.S. presidential election and the abuses that did happen on our platform.

With respect to regulation, the second one I would speak to is our Canadian integrity election initiative. As I mentioned in my opening statement, there is a report by the Communications Security Establishment that talked about the potential cyber-threats to the next federal election. There are a number of things in there. For two of them, we clearly had a piece of the responsibility for—again, cybersecurity and misinformation. Again, I just want to respectfully submit that we are not waiting for regulation. We are taking action now to address this well in advance of the federal election.

Maybe I'll turn it to Rob about—

The Chair: We're at the time, Mr. Chan.

Next up, we have Mr. Picard for seven minutes.

[*Translation*]

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

Mr. Sherman, Mr. Chan, I would like to move away from the sensational and scandalous side of the problem, while not understating how important and how serious it is.

So I would like to do a familiarization exercise with you on the situation at its most basic, so that people can really understand what we are talking about. Later, we will get back to the matter of the end user, Cambridge Analytica.

As a starting point, let me put a very simplistic deduction to you. It would seem naïve to me to think that Facebook has invested hundreds of millions of dollars simply to let people use an album—a word that the older ones among us will understand—an electronic album in this case, containing photographs of one's daily relationships and activities. It is an effective means of communication and you do not need to buy stamps or talk directly to other people.

Would a company invest hundreds of millions of dollars simply so that people can chat among themselves? I do not feel that that can be the ultimate goal of such an investment. The actual goal would be to have people participating in activities in a public forum, and, as a result, to gain access to a significant amount of not only public information, but information of all kinds, including about behaviour, material possessions, and so on. In my opinion, that has value and it is a product that can be sold.

Here is my first question. How do you determine the threshold at which private information becomes public information?

● (0925)

[*English*]

Mr. Robert Sherman: Sir, I think it's an incredibly important question. As you point out, our goal is to provide a service that enables people to communicate with the people, organizations, and ideas that are important to them, and to empower people to make the choices that are right for them. That's fundamentally what we—

[*Translation*]

Mr. Michel Picard: That is the entertainment aspect. People use the communication service for the pleasure of chatting among themselves at little cost. You are not in business for philanthropic reasons. You are in business to sell a product or a service. Communication is only the means by which you are able to do business. If your business does well, it is greatly to your credit.

Let me ask the question again: how do you determine the quality of those two services, the service dealing with private information and the service dealing with public information? You are selling something here. We want to know what it is.

[*English*]

Mr. Kevin Chan: If I may, sir, just to back up, I think my colleague Rob was trying to get at that, but allow me to try.

The history of Facebook, as you probably know, is that it didn't start as a business. It was a project of our CEO when he was a student, and the intent was very much, as you point out, to try to connect friends. Over time that service has evolved. The core of what we do is still very much about connecting friends and family together. I think it's fair to say that at some point there was a need to monetize the platform. Advertising became a model that worked well for Facebook.

I would point out that if you roll back time to about 2014, it wasn't clear that advertising, especially mobile advertising, would work for Facebook. I would say, with all due respect, I think very much for all of us who work there and certainly for Rob and me, there was a sense of optimism—and perhaps we put too much in—in trying to help connect the world and make the world a more informed and more trusted community. I think those things are still very much our guiding north stars today.

Mr. Robert Sherman: If I might add with regard to advertising specifically, as you point out, that it is an important part of the service in part because it allows people to use Facebook for free, but also because good, relevant advertising can be valuable to people. I think we have a responsibility to build our advertising business in a way that also protects people's privacy. For example, an advertiser can tell us that they want to reach people who are 18 and over in Ottawa who are interested in cars. Then we can deliver the advertisement to those people without providing those people's private information back.

Mr. Michel Picard: Gentlemen, stop, stop, stop, stop.

[*Translation*]

I am not talking about advertising. It is a specific question, how do you determine the difference between a piece of information that is private and another piece that is public?

It is a very simple question. If I post my holiday photographs on my Facebook page, I expect to see advertising from a travel agency that has viewed that public information. However, if I start to see advertisements connected with personal information that I have not published, it bothers me.

Who establishes the difference between what is private and what is public? That is the root of the problem. I cannot complain that a television channel has 20 minutes of commercials per hour of broadcasting. I have no choice, I have to watch them. I also expect to see advertising on Facebook, but how does that advertising target me personally? It is because, in some way, someone has defined what is private and what is public. I want to know the threshold used to determine that.

● (0930)

[*English*]

Mr. Robert Sherman: I certainly agree that there's a difference between public and private information. Whenever you post something on Facebook, you are able to choose right then and there whether that information will be publicly visible, whether it will be visible to your friends, or whether it will be visible to a narrower category of people.

One of the things we've invested in very heavily and which I think we need to invest more in, as Kevin mentioned, is transparency around advertising and, specifically to your point, the specific information or the specific interests that are used to judge what advertisements to show to people.

That means a couple of things. It means there are some things we shouldn't make available for targeted advertising at all. Second, it means that we should tell people—and we do tell people when they see particular ads—why they're seeing those specific ads. In my earlier example, if we think you're interested in cars, we'll tell you that that's the reason. Third, we need to put people in control. If they'd prefer not to see ads based on particular kinds of information, they should be able to do that as well.

Mr. Michel Picard: Thank you.

The Chair: Thank you, Mr. Picard.

Next up for five minutes we have Mr. Gourde.

[*Translation*]

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

Thank you, Mr. Chan and Mr. Sherman.

Along the same lines, Facebook has changed the world of information and the world of advertising in the last 15 years. Advertising on Facebook is done in a very sophisticated and very clever way. As an example, if I sell bicycles and I want to reach a certain clientele, I am going to advertise my shop on Facebook. It will then be possible for people in my region or my city looking for bicycles, or for information on a specific model, to see my advertisements at the top of the page. I feel that Facebook is capable of doing that kind of targeting. Is that true?

[*English*]

Mr. Robert Sherman: Yes, that's correct. The basic way that advertising works on Facebook is that an advertiser can come to us. An advertiser in your riding might be able to say they're selling bicycles and want to reach people in this area who are interested in bicycles. We would then deliver the advertisement to those people, as I said before, without telling the advertiser the specific people who would have seen it. But our goal is to show people ads that are relevant and useful to them. People tell us this is important when they see advertising. If we're using their time we want to make sure that people are seeing ads that they will find valuable.

[*Translation*]

Mr. Jacques Gourde: Let me continue.

But that advertising still targets people who have clicked on the advertisement about bicycles. Mr. Chan, are the people subsequently receiving that advertisement grouped together by artificial intelligence, or do other people do that research?

[*English*]

Mr. Kevin Chan: It's based on the signals we receive, the things you may have liked on Facebook and interest you have expressed on Facebook. We try to have some estimation of what your stated interests may be, and through that you're going to get potential advertising because you're in a certain audience that potentially likes bikes, for example. But I do want to unpack a bit what Rob was saying earlier....

[*Translation*]

Mr. Jacques Gourde: You have answered my question. Thank you.

Mr. Chan, on another matter, you said just now that politicians use Facebook. We use Facebook as a means of communication, but are there political parties in Canada that advertise on Facebook?

Mr. Kevin Chan: I am sorry, I did not hear the last sentence very well.

Mr. Jacques Gourde: As politicians, we use Facebook as a means of communication because it is very effective. But have any political parties in Canada previously bought advertising on Facebook?

Mr. Kevin Chan: That do not use Facebook?

Mr. Jacques Gourde: No, I am asking you whether they buy advertising.

● (0935)

Mr. Kevin Chan: Okay.

I do not know exactly, but I believe that it is possible that each federal party represented in the House of Commons has bought advertising on Facebook.

Mr. Jacques Gourde: So it is open. If a political political party wants to buy advertising, Facebook will sell it to them. Is that correct?

Mr. Kevin Chan: Yes.

Mr. Jacques Gourde: If a political party buys advertising on Facebook and if people click on the party's advertising message, can that party buy more advertising later that this time would encourage people to go and vote during an election campaign, for example?

The people who click on the advertisements, whether for the Liberal Party, the NDP or the Conservative Party, are they categorized in any way? Can people receive different advertising depending on whether it comes from the advertiser or from clients?

[*English*]

Mr. Kevin Chan: Our ad products have some functionality. If the individual, the party, or the organization chooses to, they're able to ask—for those who have expressed an interest in my advertisement—if they can reach that same audience again. To be very clear, you will never know who these individuals are. So you can never go back and say specifically you want to reach Mr. Sherman, but you can say for people who commented on my post or liked my post, I would like to reach that same audience again. You have that ability if you choose to avail yourself of it. Yes.

[*Translation*]

Mr. Jacques Gourde: Mr. Chan, I understand you cannot target people, but the political party did not necessarily ask for that. The political party wants to reach those who have clicked on a party's advertising. Does Facebook directly offer a service that involves targeting those who might have an interest in a political party in particular, or is that done by a third party?

That can change everything. People say that Facebook has changed the world of information and the world of advertising, but the platform is actually also in the process of changing history. It really can influence a critical mass of people, which can change the outcome of an election campaign that might be very close. Facebook is now an integral part of our society, a social network that is influencing people's life choices. You bear a heavy responsibility. If you provide this service, it must be provided equally to everyone. If some developers have found a way to go further than the parties can, it can greatly influence the result of a vote and influence the general direction in which society is going.

How will you be able to be on the lookout for that or to provide equal services to everyone? If developers are able to open a window to get into Facebook and plug in their app, it means that they have access to a host of data that could be distributed to a third party and not to everyone. How will you go about protecting us from that.?

[*English*]

Mr. Kevin Chan: Well, sir, just to be very clear—

The Chair: Mr. Chan, we're well over time, so make it a short response.

Mr. Kevin Chan: Oh, I'm sorry.

With respect to that, we treat all advertisers on Facebook equally, and they have access to the same products and the same services. I think I'll leave it at that.

The Chair: Thank you, Mr. Chan.

Next up, for five minutes, Mr. Saini.

Mr. Raj Saini (Kitchener Centre, Lib.): Gentlemen, good morning to you both.

The other committee I sit on is the committee on foreign affairs and international development and, in January 2017, I had the opportunity to visit Latvia ahead of our troops being deployed there. One of the things we were briefed on was the disinformation campaign that would emanate prior to our troops going there, which turned out to be true.

There were many accusations levelled against our troops: that the entire deployment was gay; that they were working to turn Latvian kids gay; that they were training neo-Nazis. For me, that's a concern, because it puts the troops at risk. This reminds me of the pizzagate scandal that happened in the United States.

What are you doing to stop the spread of this information on your platforms, and how quickly are you able to react to that kind of misinformation, especially when lives are on the line?

Mr. Kevin Chan: Thank you very much, sir, for that question.

Obviously, I think, just to roll back a bit, looking at what happened in the U.S. presidential election, we were clearly slow to react to this. We were slow to get on top of it. I want to assure you that we're now putting in all of our efforts to address this challenge head on.

I'm not familiar with the particular example you gave. But if I may, I can give you in general terms how we think about the challenge of misinformation. It turns out, upon study and research on this phenomenon, there are two things that we've identified. One is the sort of classic clickbait, low-quality content misinformation. People may not have a particular political objective, but they're going to put stuff online; they're going to try to put stuff on Facebook. The intent is to have people click to a site where they're publishing very low-quality, potentially fake information, and get people to click through until then they monetize.

A lot of this turns out to be financially motivated. What we're trying to do, using new technologies like machine learning, the artificial intelligence that we talked about earlier, is to identify this kind of behaviour, and through our signals being able to prevent them from using Facebook ads, so effectively drying up the financial incentive to cause mischief.

● (0940)

Mr. Raj Saini: I can appreciate the position that Facebook is in, with 2.2 billion users and billions of pieces of information moving on a daily basis, and I agree with that. But this was not low quality, and this affects our troops who are deployed around the world. I don't think it was done to monetize. I think it was done to spread misinformation and cause harm.

I think you're talking about two different levels. The low quality is monetization—that's fine—but there's a higher quality when you're talking about troops or other entities who are serving in different parts of the world.

I can appreciate your position because of the amount of information that's moving, but still that information has to be removed, because lives are on the line. What assurances can you give, not only to this committee but to Canadians, that troops are being protected around the world from this disinformation?

Mr. Kevin Chan: Absolutely, we take that very seriously, sir. Certainly trying to protect people and prevent real world harm is obviously paramount to what we do on our service.

On specific cases like that, we have a set of community standards that I think makes very clear that things we can all agree on should not be on the service, so no hate speech, no incitement to violence, no pornography, no terrorist content.

With what you're talking about—again, I'm not familiar with the specific instance—if this were reported to us and found to be in violation of these community standards, and it would appear from what you're saying that this was in fact the case, we would take it down. We have tens of thousands of people working on safety around the world, and a good chunk of those people focus on precisely what you're talking about.

Mr. Raj Saini: It's currently still up, but I want to move to another point. I don't have that much time.

BBC recently reported that Facebook is requesting that the Canadian–European users grant them permission to use facial recognition software to identify them in photos and videos. This is an opt-in, not an opt-out service.

Given recent activities, how can we have the confidence that this new data will be handled properly? Part of this issue is to also create new friend suggestions. How exactly will it work? What will be the primer surrounding this?

Mr. Robert Sherman: As you point out, face recognition is a feature that we're rolling out in Canada. It's something we've offered in many parts of the world for quite some time—probably around six years at this point. The primary use of face recognition technology is to suggest that people tag each other in photos. For example, if I upload a photo of Kevin, I might get a suggestion to tag him. That enables him to know that the photo exists, take action if he wants to do that, report it to Facebook if he has a concern, and all those things. We've also expanded our use of face recognition to enable people to better manage their identities so that, for example, you know if somebody's impersonating you, you know if somebody has posted a photo of you and they haven't tagged you, and also for accessibility purposes.

Mr. Raj Saini: Because this is an opt-in feature, the GDPR has tried to limit pre-ticked boxes for opt-in consent. In this case you would have to tick the box to say you don't want to be part of it, but then you'd have to go into the managed settings to reconfirm that. Is that not a bit much? If somebody consents or doesn't consent, why do they have to go through the second step to confirm that? Why is the first step not sufficient? A lot of people may not know they have to take the second step to confirm what they wanted to do in the first step.

Mr. Robert Sherman: We think it's important to be clear with people about how we use technologies as a part of Facebook, including face recognition. Our plan as we roll this out—

Mr. Raj Saini: Right, but it isn't clear, because if you tick the box —

The Chair: Your time is well past, so just quickly finish your answer, Mr. Sherman.

Mr. Robert Sherman: Our expectation is we will tell people how we're using face recognition technology. They'll have the opportunity to make one of two choices. The boxes are of equal prominence. One is to say they accept it, and they want to agree. The other is that they want to make a different choice. People will have equal ability to choose either one.

Mr. Raj Saini: It will just be one step.

The Chair: Thank you, Mr Saini.

Next up for five minutes is Mr. Kent.

Hon. Peter Kent: Some observers and critics might say the Facebook business plan is out of control. In the absence of the regulations and protocols you're now developing—that Mr. Zuckerberg said in Washington last week the company is now developing—would Facebook consider downsizing or resizing the company to something closer to its original form in order to eliminate some of the issues with third-party advertising and vandals who are abusing the system one way or another with disinformation, or fake news, if you will? It's a serious question. It would be a costly question, absolutely, for Facebook, but might it not be time for Facebook to downsize its business plan to more effectively protect user privacy?

● (0945)

Mr. Robert Sherman: It's important for us to invest very heavily in protecting user privacy and, to some of the other questions that have been asked today, to take steps to ensure integrity on the platform. I'd say two things about that. The first is that you're right that we need a focus, and particularly across the company what we've tried to do is to get people who work on our products and services—not in the context of the Facebook platform, which we're talking about today, but in other areas as well—to focus their work on promoting integrity, protecting people's data, protecting people's experiences, and promoting our broader obligation. Certainly we need to focus in that way.

As a part of our broader obligation, looking across Facebook developers and other third parties that we have relationships with, in the category of Mr. Kogan for example, we're going to have to invest very heavily in additional personnel and processes to make sure we have oversight in those areas as well.

Hon. Peter Kent: Mr. Chan.

Mr. Kevin Chan: One way to look at it and the things that Rob went through in his opening statement is to say that the process we're engaged in is very much locking down the platform. In a way, what you're talking about is making sure certain things.... We already made significant changes in 2014, as Rob mentioned, but even today, subsequent to the Cambridge Analytica news reports, we are doing a whole bunch of things not only retroactively to look at what happened with these apps, but also prospectively to change the way apps work on Facebook and drastically limit the amount of information they can get. That's just right.

The other thing I should just point out is that obviously our CEO has been very clear that this is going to be a significant investment. We expect a material impact on profitability. I think he said that, but I just wanted, again, to make that clear to the committee as well.

Hon. Peter Kent: Some of my colleagues have been talking today about the complexity and volume of material involved in acceptance clicks and opting in and opting out. For years the voices from academia and the tech world were largely ignored when they cautioned users about the way they access and what they access, and what the contract is when they click the accept box and basically agree to gain a user adventure or a good user application at the expense of revealing their personal privacy in greater or lesser amounts.

Do you think it's time now to simplify the cautions? Or is there a need for greater public education, perhaps even in schools, warning people who are going to use social media about the dangers, pitfalls, and traps they may encounter in rushing to click acceptance to gain use?

Mr. Robert Sherman: I think we at Facebook, and actually we as a broader society too, should be investing in more ways of communicating with people about privacy, rather than less. One of the things that I know the Privacy Commissioner of Canada has emphasized is that there are different kinds of uses of information that require different kinds of notice, and some uses are more sensitive than others. I certainly agree with that sentiment.

I think the way we've approached this at Facebook is to provide more detailed information in places like our privacy policy, so that people who want to dig into the details of how information is used and how they can control it can do that, and also to communicate on a day-to-day basis with people outside of the privacy policy, in ways that are maybe more accessible, about specific information, such as how to control who can communicate with you and how Facebook uses information as a part of delivering ads and how you can control that, etc. I think all of those are important.

I think your idea of doing communications within schools or in communities to help people gain literacy and the ability to make choices that are right for them is a thoughtful one, and I think that's something we should take on board.

● (0950)

Mr. Kevin Chan: If I may just add to that, on the specific thing about reaching out to the broader ecosystem and working with partners, certainly we do that in Canada with MediaSmarts, as I mentioned, which is Canada's digital literacy organization. They work closely with schools in classrooms across the country. I think that is an important ultimate backstop.

That's not to say that we don't have responsibility on our part, and I think Rob was very clear. Not only have we historically done this, we're doing more. I think the recent controls we've announced make it even easier. Before this, I think you had to go to potentially up to 20 different screens to control your experience on Facebook. We're now centralizing all of that in one map, if you will, where you can play with all the dials and have complete control over your experience and your privacy on Facebook.

We completely agree that it's very important, and we are moving to roll that out, not just in Canada but around the world.

Hon. Peter Kent: Thank you.

The Chair: Thank you, Mr. Kent.

Next up for five minutes is Ms. Vandenbeld.

Ms. Anita Vandenbeld (Ottawa West—Nepean, Lib.): I want to thank both of you for being here. As you know, this is really a crisis of confidence that many Canadians feel. It's a medium that we're using in our social interactions and to gather information and news, so I appreciate your answering the questions.

I do have some concerns regarding some testimony that we heard in our last meeting from Mr. Chris Vickery, who is an expert in data breaches. He referenced that there was another Facebook breach involving about 48 million records. He alluded to the point that this could even involve Messenger, where people's most intimate messages to one another in a private setting may have been breached. It was testimony that we heard just two days ago, but are you aware of this potential breach? Is it possible that there could be others?

Mr. Robert Sherman: I think certainly we've said that we intend to undertake an investigation with regard to Cambridge Analytica and the situation there. We need to understand what happened and where that information went. If it's still out there, we need to make sure that it's taken care of.

With regard to other situations, I think you're right: it's possible that there are other situations out there. The one that I think you may be referring to is a situation of scraping, where even public information that's available on Facebook and on the Internet was collected by a party. If that was done, that was in violation of our policies, and I think that's another area where we have taken steps but need to take more steps.

I think it's certainly a possibility that there are other incidents out there. It's incumbent upon us to do the work to understand those and mitigate them.

Ms. Anita Vandenbeld: We are talking about one app that Cambridge Analytica was using for information. There are hundreds of apps. We see invitations every day on our Facebook feeds. You're talking about 272 people who joined one app, and that affected 600,000 people. With all the other hundreds of apps out there, how big might this problem actually be?

Mr. Robert Sherman: That's something we need to get to the bottom of. We have undertaken already an effort to look back at apps that would have had access to that level of data prior to locking down our platform in 2014. We're in the process of doing that. We don't have firm answers on exactly what the scale of the problem is at this point, but it's something that we do need to undertake and that we're working to do expeditiously.

In addition to looking backward, we have an obligation to look forward, and that involves really three things. The first thing is making sure we are locking down the information that is available, so going forward, the type of information that was available previously won't be available.

The second thing is, for the limited information that is available, we need to make sure we're exercising effective oversight and that we're understanding who has that information and what they're doing with it.

The third thing, as we've talked about earlier today, is communication. We need to commit, and we have committed, to communicating much more quickly and much more practically with people when these situations arise.

Ms. Anita Vandenbeld: On the oversight piece, the second piece you mentioned, I noted that in your opening remarks you said that apps that have information will be removed after three months, that permissions will be revoked if it looks as though they're being abused. However, our committee has heard that once somebody has access to this large volume of information about an individual, they can create psychosocial behavioural profiles of that person, so that even, for instance, in the case of Cambridge Analytica, if the information has been returned to Facebook and deleted from the servers, it doesn't matter anymore because they have that behavioural profile, which then could be in the hands of anybody.

How do you prevent that from happening, and how do you make sure that flow of information is stemmed to begin with?

Mr. Robert Sherman: There are two answers to that. One is a policy answer, and one is an enforcement answer.

With regard to the policy piece, it was at the time, and continues to be, a violation of our rules for a developer to use information in that way. It would restrict both their use of the information that they directly receive from Facebook, as well as any downstream uses, such as the profiling that you are talking about. Those would both be violations of our rules. We're undertaking to investigate that ourselves.

We understand that the Information commissioner in the U.K., which has jurisdiction over Cambridge Analytica, is undertaking an investigation, and we're co-operating with that. We understand that the Privacy Commissioner in Canada is doing so as well, and we're co-operating there. We need to co-operate with both of those investigations and understand what's happening.

With regard to enforcement, after the regulators who are undertaking the investigations have told us that it is safe for us to do so, one of the things we need to do is to understand whether any of that downstream data exists. If it still does, we would take the position that it's just in the same category as their earlier data and needs to be deleted as well.

● (0955)

Ms. Anita Vandenbeld: I have one more question. I know I have limited time, but who owns the data that is put on Facebook? Obviously the public data is public domain, but when you have a message that you're sending to someone, you put your photos to friends and family only, who owns that data?

Mr. Robert Sherman: If you put information on Facebook, you own that data, and that is stated explicitly in our terms of service.

Ms. Anita Vandenbeld: Therefore, you can remove that data at any time, and be notified if somebody else is using that data. Is that something you're looking into?

Mr. Robert Sherman: That's correct. If you put data on Facebook and you want to delete it, you can delete that specific piece of data. As we referred to earlier, you can delete your account entirely and remove all the data in your account, if that's what you want to do.

One of the lessons we have learned as part of this is communicating more proactively with people if their data is misused, and that's something that we intend to do as well.

Ms. Anita Vandenbeld: Thank you. I am out of time, but hopefully I'll get another round.

The Chair: Thank you.

Next up, for a three-minute round, is Mr. Angus.

Mr. Charlie Angus: Thank you very much.

We've been talking about the data breach and the corporate culture at Facebook in response to it.

Mr. Chan, I would like to talk a bit about the corporate culture of Facebook Canada, because you're very busy in terms of outreach. You've met with election minister Gould, Minister Morneau, Minister Duncan, Minister Joly, Minister McKenna, and Minister Carolyn Bennett, who said she was absolutely inspired by your wise and frank counsel, which is very impressive.

Mr. Kevin Chan: I want to thank the minister. That was very generous.

Mr. Charlie Angus: She's a wonderful woman. I can see that, but you're not registered to lobby and none of your staff at Facebook Canada is registered as lobbyists. Why not?

Mr. Kevin Chan: Well, sir, thank you for the question.

This question does go to the heart of the company's integrity and, quite frankly, my integrity personally. I appreciate the opportunity to address this head on, if I may. At no time has Facebook come close to meeting the threshold for registration as a lobbyist. We review this posture—

Mr. Charlie Angus: It's the 20% loophole.

Mr. Kevin Chan: —on a monthly basis, sir, and will, of course, register if and when we meet the threshold.

Mr. Charlie Angus: The lobbying commissioner has raised a red flag about that threshold many times. If you're a company—and I talk to companies all the time—you hire someone who comes from the governing party. You were with the Liberal Party. You hire someone who knows the inner workings. Your experience is with the Privy Council Office. You don't have to waste your time with the drudgery of doing 20% lobbying. You just call up Minister Morneau and he's going to meet with you, so you don't ever have to meet that threshold. However, other companies, out of prudence, register because they recognize that what they're doing is lobbying. That's what you were doing: you were lobbying ministers. Why don't you follow the standards? Google, Amazon, and every other company registers to lobby. Why does Facebook think these laws are quaint?

Mr. Kevin Chan: To be clear, the meeting you're referring to with Minister Morneau, with all due respect to all parties involved, was a result of his office reaching out to Facebook. He wanted some advice on how to do Facebook Live for his budget speech.

Mr. Charlie Angus: I get that, but you are registered as the company's leading public policy-maker in Canada, "facilitating an ongoing dialogue...on a broad range of issues that impact the Internet sector". I mean, if my light bulb breaks, I don't call the head of General Electric to come to fix it, yet you show up to help him figure out how to get more "likes". Isn't that a waste of your time?

Mr. Kevin Chan: If you play it out that way, that is what I spend my time doing. I'm proud of it—

Mr. Charlie Angus: I know that, but you have enormous access. You're very friendly with these people. Why would we expect government to regulate you when you're so nice? It's nothing about Facebook, but no company wants regulation. That's why they come to meet us all the time. That's why we have rules, because they want to limit the effect of government to put the squeeze on them. Then you go and help a minister set up their Facebook page, and they aren't going to be less likely to want to regulate you. Why not just do what other companies do, and register as a lobbyist?

Mr. Kevin Chan: We'll certainly take that under advisement. Again, we do not meet the threshold.

Just to be clear to committee members, with 23 million Canadians on Facebook, and two billion globally, people use the service in many different ways. That gives rise, as we're discussing today and in other realms, to very novel public policy challenges. In fact, most of my time is spent working with a broader ecosystem to deal with these novel challenges. You have alluded to some of these institutions—

Mr. Charlie Angus: Yes, but California Facebook paid into PACs. You guys do public pressure. You do reach out. You are doing political work when you do your work. I think you should just register.

● (1000)

The Chair: We are out of time. Mr. Chan, could you quickly answer that?

Mr. Kevin Chan: We work with academics, NGOs, civil society, cultural organizations, indigenous groups, chambers of commerce, and small businesses. We build partnerships with people around the country. This is what it means to do public policy at Facebook, and I'm very proud of that.

Thank you for that feedback, and we will certainly take that under advisement.

The Chair: We're going to get to another round. I'm going to warn the committee that we have potential votes coming up. We're watching that.

We'll start the schedule again for the second hour, but we'll keep you informed there. We'll try to get as many questions in as possible.

First up for the Liberal Party is Mr. Baylis. You have seven minutes.

Mr. Frank Baylis (Pierrefonds—Dollard, Lib.): Thank you for being here, gentlemen. We appreciate it.

The challenges you have at Facebook are these. It's such a global company, it has such a global reach, and it obviously has these great strengths, but there are also challenges that come with that. One of them is jurisdictional challenges. We have our PIPEDA laws on privacy. The European Union has now put in a set of laws. The United States has laws. Some countries have no laws. Going forward, how are you going to mesh all these different laws as they come on board to ensure that Facebook is meeting and respecting the different privacy laws of different jurisdictions?

Mr. Robert Sherman: It's an important question. First, it's important for us to make sure we are giving a high level of privacy protection to everybody on Facebook, regardless of where they live. Second, it's important because individual people have different preferences as well. We need to make sure we give effect not just to national expectations, but also individual expectations.

As was discussed before, Facebook is based in California, so our primary regulatory relationship for Canadians is served by Facebook Inc. here in California, and our primary regulatory relationship is with the FTC. We also have an affiliate in Dublin that's regulated by the Irish Data Protection Commissioner—

Mr. Frank Baylis: I understand that, but as a Canadian—and I'm a Canadian—using Facebook, my data is located in the United States, and I'm protected by the United States' law, but am I also not protected by Canadian law?

Mr. Robert Sherman: That's an important question. I think it's something I personally, and we as a company, spend a lot of time on with the Canadian Privacy Commissioner. Over the course of our history many of the privacy improvements that we've made have been borne out of our discussions and investigations by the Privacy Commissioner in Canada. I think our engagements in Canada, particularly around privacy regulation, are quite important.

Mr. Frank Baylis: I'm glad that you're engaged, but I'm just curious about a very specific question. As a Canadian, if I make these laws, and yet my data and my contract per se sits with a company, Facebook, in the United States, am I protected by United States' laws or Canadian laws, and/or both, or what?

Maybe Mr. Chan can answer. Sorry, go ahead first.

Mr. Robert Sherman: I may not be the right person to answer that question. I think I would say that with regard to Facebook Inc.'s activities globally, we're regulated by the FTC. The scope of the Privacy Commissioner of Canada's jurisdiction is a question for the Privacy Commissioner, I suspect.

Mr. Frank Baylis: It's obviously your company. I would assume that you need to be aware of what laws you are or are not subject to. In your estimation, are you subject to these Canadian laws? Am I protected by these Canadian laws?

Mr. Robert Sherman: Go ahead, Kevin.

Mr. Kevin Chan: There's a bit of a lag because we're talking past each other.

Certainly you are protected by PIPEDA. Let me just find a different way to explain. We have had a longstanding relationship with the Privacy Commissioner of Canada. The Privacy Commissioner of Canada will investigate us, as they are doing right now, for things that may come in conflict with PIPEDA. We fully co-operate with the investigation, and we have, I think, implemented—

● (1005)

Mr. Frank Baylis: I do believe you're trying to act in good faith, and I'm not questioning.... I really do see the challenge that Facebook, and we ourselves in our role as writers of laws, face. I'm just trying to understand this. If we write these laws....

It's a tough question to answer, I get that; and you're going to have this coming from a number of countries, obviously, not just Canada or the U.S., but Latin America, Africa, wherever. Are you going to be taking the laws of Canada and saying, “Okay, these are Canadians and we had better make sure, however we work, that we are going to match Canadian laws”? That's a big challenge, I get that, but are you going to be doing that? Are you trying to do that?

Mr. Kevin Chan: Absolutely, sir, and it's not just in the privacy realm. There are many other areas that we touch on in how we operate or how users use our service, and we always want to be doing it in a way that is consistent.

Mr. Frank Baylis: You don't have to give me the answer now, but I would like to hear back formally as to what level you are or are not subject to our Canadian privacy laws.

Mr. Chan, you touched on the other point I wanted to talk about, which does concern me tremendously. We've seen bad actors use Facebook and other mediums, like Twitter, to interfere with democratic elections. In Canada, we have laws that control how much money can be spent to promote one party or another. I'm not attacking any particular country, but, say, a country that didn't want to follow these rules were paying someone or buying advertising and breaking our laws, but were doing it in this foreign country, what do we need to do, as regulators, as writers of law, to make sure this does not happen? It's even if they're not paid. Let's say someone is just actively flooding your social network with information and impacting our democracy for nefarious reasons. How are you going to look at this challenge? It's a huge challenge. I want to understand what you're going to do to help address that.

Mr. Kevin Chan: Sure, I'd be happy to do that.

I can obviously only speak for how we think about it at Facebook. I don't want to make representations for other companies. Again, it is clear that we were much too slow to identify this new kind of threat back in the U.S. presidential election. When we did turn our mind to it—and I was getting at it a bit with an answer to Mr. Saini—we were trying to look at automated signals to understand, from a political standpoint, foreign interference, and how we could recognize that on the platform. It turns out that it's people setting up fake accounts on Facebook and spreading misinformation.

Now, as you know, on Facebook we have an authentic identity policy. Overwhelmingly, the two-plus billion people on Facebook actually behave a certain way because they're real people. They will do things in their personal time that we expect normal people to do. The fake accounts actually behave very differently. With AI we are able to identify, and we're getting increasingly better at identifying, these fake accounts and taking them down proactively. When you look at the subsequent elections after the U.S. presidential election, when you look at the French election and the German election, and most recently at the Italian election, you will see that we were able to identify tens of thousands of fake accounts and take them down proactively. I'm pleased to say that, although, again, our work is never done—

Mr. Frank Baylis: I have a quick question before I run out of time.

Specifically on paid advertisement—and I understand how you're going to use it to find fake users and that—we control what can be done within Canada's borders in Canadian elections. If someone's buying an ad outside of our jurisdiction, but it's designed to impact our democracy.... You don't need to answer now, but I'd like to get you to think about that. Think how can we work together and what laws we need to put in place so that does not happen.

Mr. Kevin Chan: Thank you for that, sir.

We are doing a lot of thinking on that. We've made commitments for the U.S. mid-terms coming up, and I'd be happy to share them with you.

The Chair: Thank you for that.

Next up for seven minutes we have Mr. Kent.

Hon. Peter Kent: Thank you, Chair.

Mr. Chan, I was pleased to hear you acknowledge today that Facebook was too idealistic, I think you said, on how technology was used. You committed to say that, if Facebook finds abuse in the future, you will act fast and you will ban those privacy abusers.

However, some might say that's a little bit like closing the barn door after the horse has escaped, that it's an imperfect remedy, that, depending on the speed and your ability to detect abuse, much more potential abuse could be done, if for an increasingly shorter period of time.

How do you address that?

● (1010)

Mr. Kevin Chan: Are you talking in general, sir?

Hon. Peter Kent: Well, to your point about if you find abuse, you'll ban it.

Mr. Kevin Chan: Yes.

Hon. Peter Kent: You have discussed some preventive technologies, but the fact is that there's still a barn door context if you're waiting until the abuse is detected.

Mr. Kevin Chan: Yes, I better understand the question now, sir.

Again, we do have proactive measures in place that are getting increasingly better and sophisticated. Those are the AI tools I've talked about for us to be able to proactively delete accounts before mischief arrives. Again, we have looked at elections subsequent to the U.S. presidential one, for example, the German election. Independent studies have shown that the phenomenon of misinformation and fake news was not a material concern in that election.

In response to the broader point you may be raising, I just want to assure you, to the best that I can, obviously, as an individual, that we in Canada take abuse on the platform very seriously. Obviously the ones that would potentially occur during an election are the most serious.

Mr. Chair, if I may, I have a letter from the Commissioner of Canada Elections from 2016 following the 2015 election. He writes about his appreciation for the way in which Facebook Canada has engaged with his office proactively to ensure that there was no malfeasance during the last federal election. This is obviously something that we have not discussed, but I would be pleased, Mr. Chair, to circulate this letter, so people can see that—

Hon. Peter Kent: Certainly, afterwards.

Mr. Kevin Chan: —our good faith has been long-standing, and we've been applauded for it.

Hon. Peter Kent: We appreciate that. Certainly in the context of 2015, the commissioner may well have had congratulations to appropriately deliver. After Cambridge Analytica and AIQ, as you've heard, the Privacy Commissioner has some very serious concerns about how urgent it is to address these problems between now and the next federal election, let alone a number of provincial elections.

Some observers thought that in his testimony last week, Mr. Zuckerberg dodged a couple of important questions, particularly with regard to who owns virtual reality, the virtual you, if you will. His response on a number of occasions was to note that the user owns all of the content, that one uploads it and can delete it at will, but that didn't answer the question of whether the advertising profile that Facebook builds up about an individual user can be deleted The fact is that Mr. Zuckerberg didn't acknowledge that a user has no control over that data.

Mr. Robert Sherman: Sir, I can answer that question. Yes, as I mentioned earlier, I think it's important that in our terms of service the information you put on Facebook is your information. You can delete it; you own it.

With regard to the information that we use for advertising, I think it is equally important that we tell people what that information is. If you've liked the pages of several car manufacturers, we might assume that you're interested in cars. That's an assumption that Facebook has made. It's important for us to tell you about that, to give you access to that information, and to allow you to remove it, if that's what you want to do. Again, with regard to that kind of information, I think it's also important that people have access to it and be in control.

The ultimate control is that, if people don't want us to have any information about them, they can remove their account. We hope they won't do that. As we've said today, we hope we provide great value for people and the lives of every Canadian who uses Facebook. We want to make sure that at each step of the way people are in control of their information.

Hon. Peter Kent: Thank you for that.

There was one other suggestion—well, there were a number—that Mr. Zuckerberg might have dodged a couple of questions with regard to the information, the data, that Facebook holds on browsing activities. I guess he rebuffed the question. He rejected the question that Facebook does own users' browsing activity. His answer was that browsing information is not part of the user's content since the user didn't upload that information. That may well be, many observers have said, and I tend to agree with them, but that's beside the point.

So, who does own the browsing information and browsing activity of a user?

● (1015)

Mr. Robert Sherman: If I might provide one minute of context on what we're talking about.... If a website or app developer wants to integrate Facebook technology, they have the ability to do that. For example, if they want to put the Like button on their page, if you load the web page, your browser will send a request to Facebook servers to ask to receive the Like button, and then we'll obviously record that we have that information.

With regard to that information, we're using it predominantly to provide the Like button and to make sure that if you hit the Like button this is recorded in your profile. Also, it's for technical purposes to support advertising and in other ways.

With regard to that information as well, it's important that people have access to control it if they don't want that information to be used for advertising. They should be able to do that. Our practice is to delete and de-identify that information on a routine basis, independent of whether people exercise that.

Hon. Peter Kent: Do you not agree that it might be appropriate to protect users who are small "i" ignorant of what might be happening with their browsing activity or when they click that access box? Do you not agree that perhaps you should have a very clear warning—a very concise, one-sentence warning—about the dangers of unintended use of this browsing activity? Or would you not do that because that might compromise and reduce your revenue potential with these third parties?

Mr. Robert Sherman: No, I think it's important for us to let people know how this technology works. We've done that in a number of ways over the years. I think it's clear that we need to do more of that. One of the things that we've announced this week is that we're going to be educating people, specifically as a part of using the Facebook service, about the fact that this technology exists and that we collect this information. We'll be educating people in other ways as well.

We recently published a blog post on our website that provides more information about this practice. Following the hearings this past week, people were interested in understanding more.

I certainly agree with your point that we need to communicate more about this.

Hon. Peter Kent: Thank you.

The Chair: Thank you, Mr. Kent.

Mr. Angus, you have seven minutes.

Mr. Charlie Angus: Thank you.

When I was elected in 2004, I came out of the music business at a time when what was happening in Silicon Valley was turning the music industry upside down. Certainly, the massive losses in recording revenues were noted. There was a lot of pressure at that time here on the Hill to bring in legislation to regulate, to try to limit, digital growth. I was very much against that because I saw the potential for new ideas and for development, even though it was upending the music industry. Now it's upended newspapers and so many stable sources.

However, what we've seen is that so many of these young start-ups have become monopolistic giants. The idea that there would be a whole series of competing, for example, platforms has disappeared. Looking at it in 2018, my concern is that Facebook has morphed from a place where you meet your old friends from high school into the single, defining source of information for the vast majority of people. It is the news media for the vast majority of people, whether it is false news, Russian troll bot news, or CTV.

When Mr. Therrien came here the other day, he said that he needed the tools to be able to go in without permission and investigate or audit Facebook on privacy. He also raised the larger issue, that there are Competition Act issues and a series of effects that Facebook now has that have not not really been looked at.

Mr. Chan, if a federal auditor for digital platforms was brought forward who had the power to investigate these complaints to ensure compliance, what would Facebook think of that?

Mr. Kevin Chan: Sir, are you referring to privacy or something broader?

Mr. Charlie Angus: Well, Mr. Therrien mentioned privacy, but obviously Facebook affects so much more than privacy. It affects the news. It affects information. It's now affecting elections and whether or not elections can be undermined, as in the United States or as in the Brexit vote. It's a question of whether or not we need to have an independent auditor. I don't see how we can regulate something as big as Facebook when you can move 1.5 billion users from jurisdiction to jurisdiction to get around laws. Would you support an auditor?

Mr. Kevin Chan: I think there are many different instruments that already exist. I think the Privacy Commissioner is investigating. I think he is already very much seized with his existing abilities under mandate or statute to understand and get to the bottom of what he has.

Mr. Charlie Angus: I guess the question is, are you a utility now? You've moved from being a really cool space, but are you basically a public utility that everyone relies on?

● (1020)

Mr. Kevin Chan: Sure, if I may say, we are a platform where there are, as you point out, 23 million Canadians on service. We take that responsibility very seriously. I think the core of your concern is whether or not we take that responsibility seriously, and we absolutely do. If I may look at one issue that you're alluding to, the news issue—again I'm very much seized with working with a broader ecosystem—there are indeed seven million Canadians every day who get at least some part of their news from Facebook. We understand that's a very significant responsibility. We understand that we are a part of that news ecosystem—

Mr. Charlie Angus: Sorry to interrupt, but I don't want to get cut off by the votes in the House.

Let's just zero in on that issue of news. On the question of Myanmar, where Facebook was the sole source of news for a vast majority of people in Myanmar, *The Guardian* and international organizations said that the use and misuse of that platform definitely played a huge role in the horrific genocide that we've been seeing there Myanmar and in the rise of hate, because Facebook was the primary source of news. The UN investigator, Yanghee Lee, said that Facebook had become a beast in Myanmar. No one thought when we started to exchange information that it could be taken over by haters and be used in such a manner, but it has. How do we prevent that atrocity from happening again?

Mr. Kevin Chan: Sir, I, of course, would not want to speak to the specific details from another part of the world, but I can you tell you, if I may, about our global approach to this.

As I mentioned earlier, we do have community standards that apply globally. Hate speech, incitement to violence, terrorist content, those sorts of things I think we can all agree should not be on the service. We do take them down proactively where we can with artificial intelligence, which, to be very clear, is not a panacea. It's getting better, but we would not sort of say that this is always going to be perfect. We also take down content that is reported to us. I think we try to do this in all the languages in which we operate around the world.

Mr. Charlie Angus: I'm on Facebook all the time. My wife says I'm married to your platform for better or for worse. The issue I see is the anti-Muslim, pro-Russian, pro-Putin, pro-Assad comments. They are derailed comments.

I'm always trying to do deal with this, but that's small potatoes compared to what has happed in Myanmar. Alan Davis, who is one of the people looking at that genocide, said:

> I think things are so far gone in Myanmar right now... I really don't know how Zuckerberg and co sleep at night. If they had any kind of conscience they would be pouring a good percentage of their fortunes into reversing the chaos they have created.

You have an enormous power with your corporation. It's unprecedented in history. With Facebook identified as one of the key sources of such horrific killings, I would think that Facebook would be so outraged that you would be begging to come to committee, not being asked to come to committee, to say, "We will make sure that this will never happen again."

So, where is that assurance?

Mr. Kevin Chan: Well, again, sir, I would just say, respectfully, in Canada....

I will circulate documents that show that before issues generally become public issues, we have long been at work with the right authorities to get things right. Again, I could just point back to the letter I have here from the Commissioner of Canada Elections, congratulating us for our efforts—

Mr. Charlie Angus: I know, but we're talking about the power of one platform to cause horrific harm and death—an unprecedented massacre. That's an incredible power.

As a corporate entity, with Facebook's response that we've heard this morning, are you equipped to deal with this kind of power, given the potential for harm as well as the potential for good?

Mr. Kevin Chan: We understand very much where you're coming from. We understand our responsibilities. I think, as I indicated in the opening statement, we did not take a broad enough view about our responsibilities. It's not enough just to build tools that people can use; we have to ensure they're not abused.

We have made big commitments to grow our safety team, going from 10,000 to 20,000 people in the next year, which is a significant undertaking for a company of a certain number of full-time employees, and we will continue to do more, both on the technical side, which we spent some time talking about, but also on having enough people on the ground to deal with all these types of issues.

I certainly would never want to say that we are perfect and that we'll get it right tomorrow, but we certainly have been on this journey for the last year or more. We see much more work to be done. I want to assure you that we will do all we can in Canada, but also elsewhere around the world, to ensure that abuses do not happen.

● (1025)

The Chair: Thank you, Mr. Angus and Mr. Chan.

I want to highlight to folks that we've gotten word that the votes aren't likely, so you don't need to be as urgent with your questions. It looks as if we're going to get as many questioners as are on the list.

Next up we have Madame Fortier.

[*Translation*]

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

A number of years ago, I was very proud to subscribe to Facebook and I was always "liking" and "sharing". But today, in the light of what is happening, I am constantly wondering what I can post. I hope that you are going to be able to give Canadians back some trust in the network, not only through what you are doing now but above all through what you will be doing in the future.

As the mother of three children who use Facebook, I think about what awaits them in the future. I also think of my parents, who could well become vulnerable because they like everything on Facebook. I really want you to understand that, in both our professional and personal lives, we now have a filter in our heads that we have to use every day when we use Facebook.

I still maintain that Facebook is an incredible networking tool that allows me to stay in touch with my acquaintances and my family and to be up to date with everything that is going on. You can understand a little how my doubts and my lack of trust are affecting me. It is important for me to tell you this, because I feel that everyone is feeling the same way, not only in my constituency, but all over the country.

Now I would like to discuss those who create apps. We talked about them a little earlier and I would like you to explain the policy on those developers you referred to. How many of them does the policy apply to and how many violations have you had in the past? Also, what did you do about the violators?

[*English*]

Mr. Robert Sherman: Thank you for you comments, and particularly about your use of Facebook. I also use Facebook very frequently to communicate with my family and friends, and find it valuable. As we've said before, we have a very significant responsibility as well to make sure that people using our service are able to use it in a safe and protected way. That's been important for a long time, but we're continuing to invest in it.

With regard to application developers, first, we have a series of restrictions on how they can use information from the platform, including that they can't ask for information they don't need to operate their apps. They can't sell information they receive. They can't use it for monetization or app networks or those kinds of things. They have to delete the information if we or somebody else asks them to do so.

As a part of the changes we made in 2014, we introduced an upfront review process, so that apps that wanted to get access to our platform and to get those additional pieces of information would have to go through an upfront review. We also do a reactive review when we identify a problem. Those steps can include removing somebody from the platform, investigating what they're doing or—

[*Translation*]

Mrs. Mona Fortier: You are telling us today that there were violations. What did you do about them?

[*English*]

Mr. Robert Sherman: We can take a range of steps when people violate our policies. These include terminating them from the platform. We can engage them informally about improving it—if it's a minor violation of some sort. We can refer them to law enforcement or take legal action. I think one of the things that we've learned, particularly with respect to the events over the past several weeks, is that we need to be more aggressive in our oversight and our understanding of when these situations occur, and also in taking enforcement action, including collaborating with law enforcement where appropriate.

Mr. Kevin Chan: Madame, the other thing we said very clearly is that, obviously, we're going to go back and look at all the apps that were in play at the time. If we do have evidence of malfeasance, we will ban the app from the platform and will notify all affected users.

● (1030)

[*Translation*]

Mrs. Mona Fortier: Do you ask app developers to register by providing a physical address or to confirm their identity? How do you go about making sure that they really exist and that you can monitor their activities?

[*English*]

Mr. Robert Sherman: We have an application process that app developers have to undertake. They have to provide some additional information about who they are and who is responsible for them. They have to connect to a Facebook account that we can identify with a real name. There are a number of steps we take to identify them. One of the things we've been doing across the platform, that we've been investing in, is further verification to make sure that we understand who we're dealing with and, as part of the efforts we've announced, we will undertake further review of developers on the platform. As Kevin said, looking back at app developers who would have had access to significant information before, as well as going forward, we want to make sure that we have appropriate oversight, not just of what people are doing but of who is doing that information collection.

[*Translation*]

Mrs. Mona Fortier: Now I want to deal with the issue of fake accounts, which we have already talked about a little. You explained how you prevent fake accounts from being created. But, in the light of what we know today about the problem, what new measures have you undertaken recently to determine or confirm an individual's identity? What other processes or mechanisms do you have to implement to ensure that fake accounts are suspended or removed from the platform?

[*English*]

Mr. Kevin Chan: There are two things. We have talked about one already, but let me just briefly underscore them. We are constantly changing and refining the way we identify fake accounts using machine learning. So again, in elections following the U.S. presidential election, we did identify tens of thousands of fake accounts for each of these electoral moments, and we put them down proactively. Again, independent studies confirmed that in the German election, this phenomenon of information being spread by fake accounts was not a driver in that election. We feel we are making progress on this. I would never want to make you think that we think we've solved it. This is a constant game of steady improvement and technical improvement. We need to do that .

More recently, in the lead-up to the mid-term congressional elections in the United States, which I alluded to earlier, we have made commitments to roll out a second phase of ad transparencies. Again, as I mentioned, Canada is the first country that we have tested "View Ads" in. We are going to bring that to the United States prior to the U.S. congressional elections. We're also going to have special additional measures for political advertising, whether it be for individuals or issue-based ads. For those ads, we have a few measures that we will implement to try to ensure the authenticity of the individual who is running these ad accounts. For example, we will make sure they upload a government I.D., and we will then confirm their address by sending them a piece of mail with a special code in it. We will launch those things first, in advance of the mid-term congressional elections. Our intention, as we've announced, is to roll this out globally afterwards.

[*Translation*]

Mrs. Mona Fortier: Thank you very much.

[*English*]

The Chair: Thank you, Ms. Fortier.

Next up for five minutes is Mr. Gourde.

[*Translation*]

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

As lawmakers, we have no doubt that Facebook is doing everything it can to remain a valuable platform. As an analogy, nuclear medicine has valuable uses, but if the technology falls into the wrong hands, it could be used to make bombs.

Facebook has become a very large company. You said that you have put measures in place and that you have hired 10,000 to 20,000 people to make your platform safe. With more than 2 billion users, a number that is certainly going to increase exponentially in the coming months because things are moving so quickly, Facebook will be one of the most popular social media on the planet.

As lawmakers, our fear is that you may lose control of your platform despite having put in place all possible measures. In fact, there could be very smart but ill-intentioned people who would like to use your platform illegitimately, for purposes other than those we are familiar with today.

Do you believe that you will be able to regain control of the situation in the short term? As lawmakers, we are not necessarily going to be giving you four, five or 10 years to prove it. You have to face major challenges and you have a heavy responsibility to act now. Are you going to move quickly?

● (1035)

[*English*]

Mr. Kevin Chan: Thank you very much for the question, sir.

You know, for good and perhaps less good, we are known for moving quite fast to get on top of things, and I think you will see, and probably have already seen in the last few weeks, that we are moving very fast to address many of the things that have been raised. Again, as I said earlier, this is not something we have done just in the last month. I would like to characterize this more as a journey that we've been on for the last year or year and a half, to roll out a bunch of different things, a bunch of initiatives, whether they be on platform, from a technical side, or new products like "View Ads", but also partnerships with the broader ecosystem to try to prevent abuse on our platform.

Again, as I said earlier, and as I think our CEO has also said, I don't think we can ever give assurances that there won't be a bad actor who does try to abuse the platform, but we take our responsibility very seriously, and we're not waiting for authorities to decide what should be done. We take all the criticism very seriously, we take all the feedback very seriously, and we're putting in place—I hope you can appreciate—very tangible, concrete measures, both on platform and off, to address this very quickly.

[*Translation*]

Mr. Jacques Gourde: Do you have any comments, Mr. Sherman?

[*English*]

Mr. Robert Sherman: Yes, I agree with what Mr. Chan said. I think it's important for us to take steps expeditiously to address some of these challenges. I think the steps we've announced with regard to platform over the past several weeks are the first of what I expect to be many efforts along these lines, and I think some of the most immediate things we can do, in addition to looking backward, are to restrict the availability of information as quickly as we can, impose oversight.

I will say, with regard to your broader comment, that we have a broad responsibility. There are people who are going.... We've been idealistic and wanted our products to be used for good. I think it's fair to say that not everybody will use them for good. We have a responsibility to get on top of that. I think we also have a responsibility to you in Parliament and the government more generally to work also with you on those problems and make sure we're communicating with you about the steps we're taking. That's something we're committed to doing expeditiously and in consultation with the Canadian government.

[*Translation*]

Mr. Jacques Gourde: We were in a period of calm. Let us hope that it will not be the calm before a storm. When there is a nice warm breeze, everything is fine. But in a hurricane, all kinds of things can happen.

We have no arrows in our quiver to help you. If you were to ask governments all around the world to come to your assistance if you lost control of your platform, the assistance would be very limited. So your responsibility is so great that failure is not an option.

Thank you.

[*English*]

Mr. Robert Sherman: Thank you. I agree, and we certainly understand that.

The Chair: Thank you, Mr. Gourde.

There's another five minutes for Mr. Erskine-Smith.

Mr. Nathaniel Erskine-Smith: Thanks very much.

Now, you've spoken about this being a breach of trust, and you've really highlighted the importance of building up the trust of your user base. That's fair, yes?

Mr. Robert Sherman: [*Inaudible—Editor*]

Mr. Nathaniel Erskine-Smith: Okay, so is it also fair to say that, in building up the trust of your users, it's incredibly important—perhaps most important—to be as open and honest as possible. Do you think that's fair? Yes?

Mr. Robert Sherman: I think that's fair.

Mr. Kevin Chan: Yes, sir. That's right.

Mr. Nathaniel Erskine-Smith: I asked about personal information being shared without consent previously, and what the most personal and most sensitive information might be that was shared without users' consent, and Mr. Sherman, you gave an example of likes. You didn't mention private messages, though, and I have a notice in front of me from an individual who did not access This Is Your Digital Life but a friend did, and it indicates that for a small numbers of users—it doesn't indicate what percentage or how many—their posts, timelines, and also messages may have been shared.

Can you comment on that?

Mr. Robert Sherman: We're still in the process of investigating and looking into the records that we have with regard to what was shared with This is Your Digital Life. As I've said previously, we want to undertake a forensic audit to look at the information that's in Cambridge Analytica's possession and make sure we understand that. It's possible that private messages were shared in small numbers as part of that. That's something that was allowed on the platform at the time.

Mr. Nathaniel Erskine-Smith: In your opinion, based on the evidence you've reviewed to date, do you think private messages were shared without users' consent?

Mr. Robert Sherman: I believe it's possible, but I think it's something we need to confirm.

Mr. Nathaniel Erskine-Smith: Okay. Who's confirming that, and when are we going to get confirmation?

Mr. Robert Sherman: We have engaged forensic auditors who would look at that question. We've been asked by the U.K. government, which is conducting its investigation, to wait until they're at a point when they're ready for us to do that, so we're co-operating with government investigations, but we also want to do our own review.

● (1040)

Mr. Nathaniel Erskine-Smith: I would like your undertaking, then, to provide this committee with a list, an example, of all kinds of personal information of individuals that would have been shared without those individuals' consent.

Mr. Robert Sherman: We are still in the process of developing that information, but we will follow up.

Mr. Nathaniel Erskine-Smith: You will follow up with us, okay. That's great.

Now, in the interest of being as open and honest with Canadians as possible, why haven't you mentioned LocalBlox today?

Mr. Robert Sherman: I'm sorry, can you explain what you mean?

Mr. Nathaniel Erskine-Smith: We had Chris Vickery before us earlier this week, who discussed 48 million additional users who had their information shared in some improper fashion. Are you familiar with the context of that?

Mr. Robert Sherman: I am, yes.

Mr. Nathaniel Erskine-Smith: Are you also familiar with LocalBlox being the company that was scraping user profiles?

Mr. Robert Sherman: As I mentioned before, the problem of scraping is one we deal with at Facebook and that any Internet service deals with. It's one of the things we announced this past week as part of a series of changes we're making dealing with situations where public information that's just generally available on the Internet is acquired in large scale. This is sort of the practice we refer to as scraping. We have technical measures in place to deal with that and to identify when that happens. For example, large-scale automated efforts to collect information is a violation of our rules. Many of the times when people try to engage in it, we detect it, but it's very clear from that example you've given that we need to do more. I think I referred earlier to some of the—

Mr. Nathaniel Erskine-Smith: Isn't it also clear, though, that you should be...? You've indicated the importance of building the trust of your user base, but the only reason you're talking about LocalBlox and 48 million users having their information scraped is that I asked you about it. It's really curious to me, when you've already indicated that being open and honest is so very important.

Are you also looking at the idea of privacy by design, which is that privacy is a default setting? If you're so concerned about the scraping of user profiles, have you gone down this road of examining what privacy by default might look like, to avoid the scraping of user profiles?

Mr. Robert Sherman: Thank you for the question. Privacy by design is extraordinarily important at Facebook. We have a cross-functional privacy program that includes experts from around the company who, as we're building products, think about data collection and data use and how we can communicate with people and put them in control.

One example is that several years back, we changed our default for sharing so that when you post something on Facebook as a new user, we'll ask you if you want this information to be made public or if you want this information to be shared only with your friends. People have the ability to change that an any time.

We've also done privacy checkups to reconfirm that with people so that people can let us know. By default, when you post on Facebook, information is shared with your friends, but we also want to give people the ability to share publicly, and unfortunately, one of the challenges is that if you post something publicly on the Internet, anyone can see it, and sometimes that includes people who are scraping—

Mr. Nathaniel Erskine-Smith: The only other undertaking I would ask is that when you have reconciled the number of applications that have improperly shared information without users' consent, and you've assessed the number of users who have been affected, you also provide that information to this committee.

Mr. Robert Sherman: Absolutely. We're in the process of looking not only at Cambridge Analytica but at other situations as well. Once we understand the scope of that problem, we will certainly communicate that.

Mr. Nathaniel Erskine-Smith: Thanks very much.

The Chair: Thank you, Mr. Erskine-Smith.

The last couple of minutes go to Mr. Kent.

Hon. Peter Kent: Thank you very much, Chair.

Mr. Chan, Mr. Sherman, this follows the point Mr. Saini made earlier at the end of his questioning. The Facebook posting of Russian disinformation maliciously attacking, or trying to attack, the credibility of Canadian Forces serving in Latvia says that it was posted “about 10 months ago”. It is still up on that site, which I think is a fairly obvious posting of malicious material that is certainly fake information that should be removed. On the other side of the coin, there are any number of complaints from human rights groups in countries like Iran, Russia, China, and elsewhere around the world that when the governments of those dictatorships, authoritarian governments, complain to Facebook about the human rights postings they make, they are too often removed.

What's Facebook doing with regard to the balance of hateful disinformation and the repression of legitimate information in some of these far-from-democratic countries?

● (1045)

Mr. Kevin Chan: Thank you very much for the question, sir. With respect to the post you referred to, if it's appropriate for me to ask if your office could follow up with me afterwards, then I would be happy to take a look at it and see what may be the issue there.

Generally, sir, as you and others have pointed out, we obviously operate around the world. We do want to be sensitive to local laws, cultures, and customs in many respects as well. I think your point very much seizes on the challenge of making sure that we are doing this in a way that ensures we have consistency, but also that we are sensitive to the realities in different countries. That's why we have a global set of community standards.

We do recognize that those are not perfect. As cases arise—and you can imagine that there are going to be, on any given day, millions if not billions of posts in a day—they will give rise, as I mentioned to Mr. Angus for a different question, to novel public policy issues. Every time we encounter these novel cases, it is once again an opportunity for us to engage and to try to understand what the right response will be.

I think that in general, sir, we obviously have very clear standards on hate speech, terrorist content, pornography, and those sorts of things. Obviously, we hear about those sorts of things and we would not want to see those sorts of things on Facebook. We take all of these things very seriously.

Hon. Peter Kent: Yes, and I think the concern is about the suppression and repression of legitimate human rights information at the direction of these questionable sovereign governments.

The Chair: Thank you, Mr. Kent.

To finish up, as chair of the committee, I'll say that I think we've all appreciated the good parts of Facebook allowing us to connect with loved ones and voters, etc., on a daily basis. I check Facebook regularly for my news, yet we task you with the deep responsibility of keeping Canadians' data safe.

I think one thing that's unique about this committee is that all parties are committed to doing what we need to do to ensure that you keep Canadians' data safe.

Thank you once again, Mr. Chan and Mr. Sherman, for your attendance today.

We're adjourned.