HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 153 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, May 28, 2019

Chair

Mr. Bob Zimmer

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, May 28, 2019

● (1040)

[*English*]

The Chair (Mr. Bob Zimmer (Prince George—Peace River—Northern Rockies, CPC)): We'll bring to order meeting 153 of the Standing Committee on Access to Information, Privacy and Ethics and by extension the international grand committee on big data, privacy and democracy. We will have countries' representatives speak as well. We'll start off with my co-chair, Mr. Damian Collins from the U.K.

The way it will work structurally is that we'll go through the delegations, one representative per country initially and then the second representative. You each should have your own five-minute time slot exclusive to yourself.

Before we begin, Mr. Angus has a comment.

Mr. Charlie Angus (Timmins—James Bay, NDP): Mr. Chair, just as a point of order for our committee, we are very surprised, I think, that Mr. Zuckerberg decided—and Ms. Sandberg—to ignore the summons of a parliamentary committee, particularly as we have international representatives here. As far as I know, we were not even informed that he wasn't showing up. I have never seen a situation where a corporate head ignores a legal summons.

In light of that, I would like to bring notice of a motion to vote on:

> That the Standing Committee on Access to Information, Privacy and Ethics, on account of the refusal of Mr. Mark Zuckerberg and Ms. Sheryl Sandberg to appear before it on May 28th, direct the Chair to serve either or both with a formal summons should they arrive in Canada for any purpose to appear before the Committee at the date of the next meeting from the date of their summons, and should they be served with a summons when the House is not sitting, that the Chair reconvene the Committee for a special meeting as soon as practicable for the purpose of obtaining evidence from them.

Mr. Chair, I don't know if we've ever used an open summons in Parliament—we've checked and we haven't found one—but I believe you'll find that this is in order. If Mr. Zuckerberg or Ms. Sandberg decide to come here for a tech conference or to go fishing, Parliament will be able serve that summons and have them brought here.

The Chair: Thank you, Mr. Angus.

For the ex officio members of the committee, we have a motion before our committee that we will have to vote on, so there will be some discussion.

Is there any discussion from any other members about the motion?

Mr. Kent.

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

Yes, the official opposition, the Conservative Party, is fully willing to support Mr. Angus's motion. As we heard in some of the previous testimony, Facebook, among others of the large platforms, has shown extreme disrespect and disregard for sovereign governments and for committees representing sovereign governments, with regard to their concerns and the search for explanations as to why meaningful action has not been taken to date and for a clear and explicit explanation of their response to the concerns from around the world and certainly within democracies and the members of this international grand committee.

We will support this motion. Thank you.

The Chair: There was a discussion previously about no substantive motions being brought before the committee. That said, with all agreement at the table here, I think we can agree to have that heard—and we are hearing it today—and voted on.

Do we have...? I see all in favour of having that motion moved before us.

Are there any other comments about the motion?

Mr. Lucas.

Mr. Ian Lucas (Member, Digital, Culture, Media and Sport Committee, United Kingdom House of Commons): This is a case of recidivism by Mr. Zuckerberg. This has happened previously, and it is a matter of deep concern. It's particularly of great concern to me, because unfortunately governments are continuing to meet with Mr. Zuckerberg, and I think it important that we should communicate, as parliamentarians, our concern about the disrespect that Mr. Zuckerberg is showing to parliamentarians from across the world. They should consider the access they give Mr. Zuckerberg, access to governments and to ministers, operated in private, without respect to us as parliamentarians and without respect to our constituents, who are excluded from the confidential discussions that are happening on these crucial matters.

The Chair: Thank you, Mr. Lucas.

Mr. Erskine-Smith.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): I would just note that it's funny that less than two months ago, on March 30, Mark Zuckerberg wrote an op-ed in the Wall Street Journal. He wrote that he believes Facebook has a responsibility to address harmful content, protecting elections, privacy and data protection and data portability—the very issues we're discussing today—and that he was looking forward to discussing them with lawmakers around the world. Those were his words less than two months ago. If he were an honest individual in writing those words, he'd be sitting in that chair today.

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

Are there any further comments on the motion?

Frankly, to answer your question, being the chair of this committee on both levels, the international and our ethics committee, it's abhorrent that he's not here today and that Ms. Sandberg is not here today. It was very clearly communicated to them that they were to appear today before us. A summons was issued, which is already an unusual act for a committee. I think it's only fitting that there be an ongoing summons. As soon as either Mr. Zuckerberg or Ms. Sandberg step foot into our country, they will be served and expected to appear before our committee. If they choose not to, then the next step will be to hold them in contempt.

I think the words are strong, Mr. Angus, and I applaud you for your motion.

If there is not any further discussion on the motion, we'll go to the vote.

(Motion agreed to)

The Chair: Thank you, Mr. Angus.

Next, we'll go to the platforms. We'll start with Facebook, go to Google, and then....

I'll mention the names. With Facebook Inc., we have Kevin Chan, Global Policy Director for Canada, and Neil Potts, Global Policy Director. With Google LLC, we have Derek Slater, Global Director of Information Policy; and with Google Canada, Colin McKay, Head, Government Affairs and Public Policy. From Twitter Inc., we have Carlos Monje, Director of Public Policy, and Michele Austin, Head, Government and Public Policy, Twitter Canada.

I would like to say that it wasn't just the CEOs of Facebook who were invited today. The CEOs of Google were invited. The CEO of Twitter was invited. We are more than disappointed that they as well chose not to show up.

We'll start off with Mr. Chan, for seven minutes.

Thank you.

● (1045)

Mr. Kevin Chan (Global Policy Director, Facebook Inc.): Thank you very much, Mr. Chair.

My name is Kevin Chan, and I am here today with my colleague Neil Potts. We are both global policy directors at Facebook.

The Internet has transformed how billions of people live, work and connect with each other. Companies such as Facebook have immense responsibilities to keep people safe on their services. Every day we are tasked with the challenge of making decisions about what speech is harmful, what constitutes political advertising and how to prevent sophisticated cyber-attacks. This is vital work to keeping our community safe, and we recognize this work is not something that companies like ours should do alone.

[*Translation*]

New rules for the Internet should preserve what is best about the Internet and the digital economy—fostering innovation, supporting growth for small businesses, and enabling freedom of expression—while simultaneously protecting society from broader harms. These are incredibly complex issues to get right, and we want to work with governments, academics and civil society around the world to ensure new regulations are effective.

[*English*]

We are pleased to share with you today some of our emerging thinking in four areas of possible regulatory action: harmful content, privacy, data portability and election integrity.

With that, I will turn it over to my colleague Neil, who would love to engage with you about harmful content.

Mr. Neil Potts (Global Policy Director, Facebook Inc.): Chair, members of the committee, thank you for the opportunity to be here today.

I'm Neil Potts. I'm a Director with oversight of the development and implementation of Facebook's community standards. Those are our guidelines for what types of content are allowed on our platform.

Before I continue, though, I'd just like to point out that Kevin and I are global directors, subject matter area experts, ready to engage with you on these issues. Mark and Sheryl, our CEO and COO, are committed to working with government in a responsible manner. They feel that we have their mandate to be here today before you to engage on these topics, and we are happy to do so.

As you know, Facebook's mission is to give people the power to build community and to bring the world closer together. More than two billion people come to our platform every month to connect with family and friends, to find out what's going on in the world, to build their businesses and to help those in need.

As we give people a voice, we want to make sure that they're not using that voice to hurt others. Facebook embraces the responsibility of making sure that the tools we build are used for good and that we keep people safe. We take those responsibilities very seriously.

Early this month, Facebook signed the Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online, and we have taken immediate action on live streaming. Specifically, people who have broken certain rules on Facebook, which include our “dangerous organizations and individuals” policy, will be restricted from using Facebook Live.

We are also investing $7.5 million in new research partnerships with leading academics to address the adversarial media manipulation that we saw after Christchurch—for example, when some people modified the video to avoid detection in order to repost it after it had already been taken down.

As the number of users on Facebook has grown, and as the challenge of balancing freedom of expression and safety has increased, we have come to realize that Facebook should not be making so many of these difficult decisions alone. That's why we will create an external oversight board to help govern speech on Facebook by the end of 2019. The oversight board will be independent from Facebook, and it will be a final level of appeal for what stays up and what comes down on our platform.

Even with the oversight board in place, we know that people will use many different online platforms and services to communicate, and we'd all be better off if there were clear baseline standards for all platforms. This is why we would like to work with governments to establish clear frameworks related to harmful online content.

We have been working with President Macron of France on exactly this kind of project, and we welcome the opportunity to engage with more countries going forward.

Kevin.

● (1050)

Mr. Kevin Chan: In terms of privacy we very clearly understand our important responsibility as custodians of people's data and the need for us to do better. That is why, since 2014, we have taken significant measures to drastically reduce the amount of data that third party applications can access on Facebook and why we're putting together a much bigger and muscular privacy function within the company. We've also made significant advancements to give people more transparency and control over their data.

We recognize that, while we're doing much more on privacy, we're all better off when there are overarching frameworks to govern the collection and use of data. Such frameworks should protect your right to choose how your information is used, while enabling innovation. They should hold companies such as Facebook accountable by imposing penalties when we make mistakes and should clarify new areas of inquiry, including when data can be used for the public good and how this should be applied to artificial intelligence.

There are already some good models to emulate, including the European Union's General Data Protection Regulation and Canada's Personal Information Protection and Electronic Documents Act. Achieving some degree of harmonization around the world would be desirable and would facilitate economic growth.

We also believe that the principle of data portability is hugely important for consumer choice and for ensuring a dynamic and competitive marketplace for digital services. People should be able to take the data they have put on one service and move it to another service. The question becomes how data portability can be done in a way that is secure and privacy-protective. Data portability can only be meaningful if there are common standards in place, which is why we support a standard data transfer format and the open source data transfer project.

Finally, Facebook is doing its utmost to protect elections on our platform around the world by investing significantly in people, technology and partnerships. We have tripled the number of people working on security matters worldwide from 10,000 to 30,000 people. We have developed cutting-edge AI technology that allows us to detect and remove fake accounts en masse.

Of course, we cannot achieve success working only on our own, so we've partnered with a wide range of organizations. In Canada we are proud to be working with Agence France-Presse on third party fact checking, MediaSmarts on digital literacy and Equal Voice to keep candidates, in particular women candidates, safe online.

Facebook is a strong supporter of regulations promoting the transparency of online political advertising. We think it is important that citizens should be able to see all the political ads that are running online, especially those that are not targeted at them. That is why we support and will comply with Bill C-76, Canada's Elections Modernization Act, which this Parliament passed, and will be engaging in the weeks ahead with Canadian political advertisers, including the federal political parties represented here today, on important changes for political advertising that will come to the platform by the end of June.

Finally, Mr. Chair, if I may, as you will know, Facebook is part of the Canada declaration on electoral integrity online, which sets out 12 commitments that the Government of Canada and certain online platforms agree to undertake together in the lead up to the October federal election. This is a strong expression of the degree to which we are taking our responsibilities seriously in Canada, and we look forward to working in lockstep with officials to guard against foreign interference.

Thank you for the opportunity.

[*Translation*]

We look forward to taking your questions.

[*English*]

The Chair: Thank you, Mr. Chan.

Next up, we'll go to Mr. Slater, with Google.

Mr. Derek Slater (Global Director, Information Policy, Google LLC): Thank you for the opportunity to appear before you today.

My name is Derek Slater, and at Google I help shape the company's approach to information policy and content regulation. I'm joined here by my colleague Colin McKay, who's the head of public policy for Google in Canada.

We appreciate your leadership and welcome the opportunity to discuss Google's approach to addressing our many shared issues.

For nearly two decades, we have built tools that help users access, create and share information like never before, giving them more choice, opportunity and exposure to a diversity of resources and opinions. We know, though, that the very platforms that have enabled these societal benefits may also be abused, and this abuse ranges from spam to violent extremism and beyond. The scrutiny of lawmakers and our users informs and improves our products as well as the policies that govern them.

We have not waited for government regulation to address today's challenges. Addressing illegal and problematic content online is a shared responsibility that requires collaboration across government, civil society and industry, and we are doing and will continue to do our part.

I will highlight a few of the things we're doing today. On YouTube, we use a combination of automated and human review to identify and remove violative content. Over time we have improved, removing more of this content faster and before it's even viewed. Between January and March 2019, YouTube removed nearly 8.3 million videos for violating its community guidelines, and 76% of these were first flagged by machines rather than people. Of those detected by machines, over 75% had never received a single view.

When it comes to combatting disinformation, we have invested in our ranking systems to make quality count in developing policies, threat monitoring and enforcement mechanisms to tackle malicious behaviours and in features that provide users with more context, such as fact check or information panels on Google Search and YouTube.

Relatedly, in the context of election integrity, we've been building products for over a decade that provide timely and authoritative information about elections around the world. In addition, we have devoted significant resources to help campaigns, candidates and election officials improve their cybersecurity posture in light of existing and emerging threats. Our Protect Your Election website offers free resources like advanced protection, which provides Google's strongest account security, and Project Shield, a free service designed to mitigate the risk of distributed denial of service attacks that inundate sites with traffic in an effort to shut them down.

While industry needs to do its part, policy-makers, of course, have a fundamental role to play in ensuring everyone reaps the personal and economic benefits of modern technologies while addressing social costs and respecting fundamental rights. The governments and legislatures of the nearly 200 countries and territories in which we operate have come to different conclusions about how to deal with issues such as data protection, defamation and hate speech. Today's legal and regulatory frameworks are the product of deliberative processes, and as technology and society's expectations evolve, we need to stay attuned to how best to improve those rules.

In some cases, laws do need updates, for instance, in the case of data protection and law enforcement access to data. In other cases, new collaboration among industry, government and civil society may lead to complementary institutions and tools. The recent Christchurch call to action on violent extremism is just one example of this sort of pragmatic, effective collaboration.

Similarly, we have worked with the European Union on its hate speech code of conduct, which includes an audit process to monitor how platforms are meeting their commitments, and on the recent EU Code of Practice on Disinformation. We agreed to help researchers study this topic and to provide a regular audit of our next steps in this fight.

New approaches like these need to recognize relevant differences between services of different purpose and function. Oversight of content policies should naturally focus on content sharing platforms. Social media, video sharing sites and other services that have the principle purpose of helping people to create content and share it with a broad audience should be distinguished from other types of services like search, enterprise services, file storage and email, which require different sets of rules.

With that in mind, we want to highlight today four key elements to consider as part of evolving oversight and discussion around content sharing platforms.

First is to set clear definitions.

While platforms have a responsibility to set clear rules of the road for what is or is not permissible, so too, do governments have a responsibility to set out the rules around what they consider to be unlawful speech. Restrictions should be necessary and proportionate, based on clear definitions and evidence-based risks and developed in consultation with relevant stakeholders. These clear definitions, combined with clear notices about specific pieces of content, are essential for platforms to take action.

● (1055)

Second, develop standards for transparency and best practice.

Transparency is the basis for an informed discussion and helps build effective practices across the industry. Governments should take a flexible approach that fosters research and supports responsible innovation. Overly restrictive requirements like one-size-fits-all removal times, mandated use of specific technologies or disproportionate penalties will ultimately reduce the public's access to legitimate information.

Third, focus on systemic recurring failures rather than one-offs.

Identifying and responding to problematic content is similar, in a way, to having information security. There will always be bad actors and bugs and mistakes. Improvement depends on collaboration across many players using data-driven approaches to understand whether particular cases are outliers or representative of a more significant recurring systemic problem.

Fourth and finally, foster international co-operation.

As today's meeting demonstrates, these concerns and issues are global. Countries should share best practices with one another and avoid conflicting approaches that impose undue compliance burdens and create confusion for customers. That said, individual countries will make different choices about permissible speech based on their legal traditions, history and values consistent with international human rights obligations. Content that is unlawful in one country may be lawful in another.

These principles are meant to contribute to a conversation today about how legislators and governments address the issues we are likely to discuss, including hate speech, disinformation and election integrity.

In closing, I will say that the Internet poses challenges to the traditional institutions that help society organize, curate and share information. For our part, we are committed to minimizing that content that detracts from the meaningful things our platforms have to offer. We look forward to working with the members of this committee and governments around the world to address these challenges as we continue to provide services that promote and deliver trusted and useful information.

Thank you.

● (1100)

The Chair: Thank you.

Next up we'll go to Twitter. I believe Mr. Monje is going to be speaking.

Go ahead.

Mr. Carlos Monje (Director, Public Policy, Twitter Inc.): Thank you very much.

Chairman Zimmer, Chairman Collins and members of the committee, my name is Carlos Monje. I'm Director of Public Policy for Twitter. I'm joined by Michele Austin, who's our Head of Public Policy for Canada.

On behalf of Twitter, I would like to acknowledge the hard work of all the committee members on the issues before you. We appreciate your dedication and willingness to work with us.

Twitter's purpose is to serve the public conversation. Any attempts to undermine the integrity of our service erodes the core tenets of freedom of expression online. This is the value upon which our company is based.

The issues before this committee are ones that we care about deeply as individuals. We want people to feel safe on Twitter and to understand our approach to health and safety of the service. There will always be more to do, but we've made meaningful progress.

I would like to briefly touch upon our approach to privacy and disinformation and I look forward to your questions.

Twitter strives to protect the privacy of the people who use our service. We believe that privacy is a fundamental human right. Twitter is public by default. This differentiates our service from other Internet sites. When an individual creates a Twitter account and begins tweeting, their tweets are immediately viewable and searchable by anyone around the world. People understand the default public nature of Twitter and they come to Twitter expecting to see and join in a public conversation. They alone control the content that they share on Twitter, including how personal or private that content might be.

We believe that when people trust us with their data, we should be transparent about how we provide meaningful control over what data is being collected, how it is used and when it is shared. These settings are easily accessible and built with user friendliness front of mind. Our most significant personalization in data settings are located on a single page.

Twitter also makes available the “your Twitter data” toolset. Your Twitter data provides individuals with insight on the types of data stored by us, such as username, email address, phone numbers associated with the account, account creation details and information about the inferences we may have drawn. From this toolset, people can do things like edit their inferred interests, download their information and understand what we have.

Twitter is also working proactively to address spam, malicious automation, disinformation and platform manipulation by improving policies and expanding enforcement measures, providing more context for users, strengthening partnerships with governments and experts, and providing greater transparency. All of this is designed to foster the health of the service and protect the people who use Twitter.

We continue to promote the health of the public conversation by countering all forms of platform manipulation. We define platform manipulation as using Twitter to disrupt the conversation by engaging in bulk aggressive or deceptive activity. We've made significant progress. In fact, in 2018, we identified and challenged more than 425 million accounts suspected of engaging in platform manipulation. Of these, approximately 75% were ultimately suspended. We are increasingly using automated and proactive detection methods to find abuse and manipulation on our service before they impact anyone's experience. More than half the accounts we suspend are removed within one week of registration—many within hours.

We will continue to improve our ability to fight manipulative content before it affects the experience of people who use Twitter. Twitter cares greatly about disinformation in all contexts, but improving the health of the conversation around elections is of utmost importance. A key piece of our election strategy is expanding partnerships with civil society to increase our ability to understand, identify and stop disinformation efforts.

Here in Canada, we're working with Elections Canada, the commissioner of Canada Elections, the Canadian centre for cybersecurity, the Privy Council Office, democratic institutions and civil society partners such as the Samara Centre for Democracy and The Democracy Project.

In addition to our efforts to safeguard the service, we believe that transparency is a proven and powerful tool in the fight against misinformation. We have taken a number of actions to disrupt foreign operations and limit voter suppression and have significantly increased transparency around these actions. We released to the public and to researchers the world's largest archive of information operations. We've pervaded data and information on more than 9,600 accounts including accounts originating in Russia, Iran and Venezuela, totalling more than 25 million tweets.

It is our fundamental belief that these accounts and their content should be available and searchable, so that members of the public, governments and researchers can investigate, learn and build media literacy capabilities for the future. They also help us be better.

● (1105)

I want to highlight one specific example of our efforts to combat disinformation here in Canada.

Earlier this spring we launched a new tool to direct individuals to credible public health resources when they searched Twitter for key words associated with vaccines. Here we partnered with the Public Health Agency of Canada. This new investment builds on our existing work to guard against the artificial amplification of non-credible content about the safety and effectiveness of vaccines. Moreover, we already ensure that advertising content does not contain misleading claims about the cure, treatment, diagnosis or prevention of any disease, including vaccines.

In closing, Twitter will continue to work on developing new ways to maintain our commitment to privacy, to fight disinformation on our service and to remain accountable and transparent to people across the globe. We have made strong and consistent progress, but our work will never be done.

Once again, thank you for the opportunity to be here. We look forward to your questions.

The Chair: Thank you.

First of all, we will go to my co-chair, Damian Collins, and then the sequence will follow.

You each have five minutes. Try to keep it as crisp as you possibly can.

Mr. Collins.

Mr. Damian Collins (Chair, Digital, Culture, Media and Sport Committee, United Kingdom House of Commons): Thank you, Mr. Chairman.

I'm going to direct my first question to the Facebook representatives. I'm sure you're aware that one of the principal concerns of members of this committee has been that deceptive information, deliberately and maliciously spread through the tools created by social media companies, are a harm to democracy, and this disinformation is used to undermine senior politicians and public figures, public institutions and the political process.

With that in mind, could Facebook explain why it has decided not to remove the video of Nancy Pelosi that presents a distorted impression of her to undermine her public reputation? The reason I think this is so important is that we're all aware that new technology is going to make the creation of these sorts of fake or manipulated films much easier. Perhaps you could explain why Facebook is not going to take this film down.

Mr. Neil Potts: Thank you, Mr. Collins.

I'm happy to explain our approach to misinformation a bit more clearly for this committee.

First, I want to be clear that we are taking action against that video —

Mr. Damian Collins: I'm sorry, Mr. Potts, we haven't got much time. I'd like you to answer the question you've been asked, not give a statement about Facebook's policies on misinformation or what else you might have done. I want you to answer the question as to why you, unlike YouTube, are not taking this film down?

Mr. Neil Potts: We are aggressively down ranking that—

Mr. Damian Collins: I know you're down ranking it. Why aren't you taking the film down?

Mr. Neil Potts: It is our policy to inform people when we have information on the platform that may be false, so they can make their own decisions about that content.

Mr. Damian Collins: But this is content that I think is widely accepted as being fake. YouTube has taken it down. The fact-checkers that work with Facebook are saying it's fake, yet the video is allowed to remain and that video being there is far more powerful than any legal disclaimer that may be written under or over it.

Why won't you say that films that are clearly fake and are independently verified as being fake, that are there to deceive people about some of the most senior politicians in your country, will be taken down?

Mr. Neil Potts: We are conducting research on our inform treatments. That is the treatment that shows that something is fake. For example, if someone wanted to share this video with their friends or if they have already shared it or when they see it in a newsfeed, they receive a message that says it's false.

Mr. Damian Collins: Facebook accepts that this film is a distortion, doesn't it?

Mr. Kevin Chan: Neil, you're closer to this, but my understanding is that the video in question has been slowed down. Is that what this is?

Mr. Neil Potts: That's correct. I think this is manipulated—

Mr. Damian Collins: It's manipulated film to create the distorted impression that Nancy Pelosi was somehow impaired when she was speaking. That's what has happened and that's why YouTube has taken the film down and that's why there has been a general recognition, including by independent fact-checkers who work for Facebook, that this film is distorted and creates a distorted impression of the third most senior politician in America.

● (1110)

Mr. Neil Potts: As you mentioned the fact-checkers, we work with over 50 fact-checkers internationally that are—

Mr. Damian Collins: This is not in question. The fact-checkers recognize it's fake. You're saying it can stay there. Do you not see that what Facebook is doing is giving a green light to anyone in the world who wants to make a distorted or fake film about a senior politician, or maybe in the future use deepfake technologies to do it, and know that whatever happens Facebook won't remove the film?

Mr. Neil Potts: I think you're asking a philosophical question, sir. Should we remove or should we inform people that it is fake? We have taken the approach to inform people that it's fake, so they can understand why that video is on the platform and what other independent parties have considered this to be. They have considered it to be false and now they see this on our platform if they go to share it. All these questions, I think are very thorough questions, but it allows people to make their own decision and it allows them to tell others it is false.

You mentioned that the video is slowed down, which by all accounts and the fact-checkers have said it is, but I think there are many different cases where videos are slowed down and that would perhaps not be a warrant for this committee.

Mr. Damian Collins: The issue here is to say that if someone is making a film, or slowing down a film or manipulating a film, to try to create the false impression that a senior public figure is not fit for office, then that is an attempt to undermine them and the office they hold.

This is not a question of opinion. This is not a question of free speech. This is a question of people manipulating content in order to undermine public figures, and my concern is that to leave that sort of content up there, when it is indisputably fake, indisputably false and distorted, and to allow permission for this content to be shared with and promoted by other users is irresponsible.

YouTube has removed this content. I don't understand why Facebook doesn't do the same.

Mr. Neil Potts: Sir, I understand your concerns, but I think your questions are the right ones and that they show the complexity of this issue and also show perhaps that the approach we are taking is working. You don't hear people—

Mr. Damian Collins: Sorry, but with all respect, what it shows is the simplicity of these issues, the simplicity that another company has taken, recognizing the same issues, the simple action to say that this is clearly fake, it's clearly distorted, it's there to undermine senior public figures and it actually shouldn't have a place on the platform. It shouldn't be part of your community.

Mr. Neil Potts: Your opinion is right, and I obviously respect the opinion of YouTube as an independent company, but we're not hearing people talk about this video as if it were real. We're hearing people discuss the fact that it is fake and that it is on the platform, so on the question of whether we have informed people that this is a fake video, yes, we have. I think that is the predominant speech right now. Whether it's the conversation we're having right now, whether it's on the news or others, people understand that this video is fake and they can make further decisions from there.

Mr. Damian Collins: My concern about this is that it sets a very dangerous precedent. Your colleague Monika Bickert said last week to CNN that basically Facebook's policy is that any political content, any disinformation content in relation to politics will not be taken down, that there would be notes put up for users so they could see that the facts are disputed, but it will never be removed.

If you're going to allow your platform to be abused in this way by people producing disinformation films targeted at users to try to interfere with democracy and the best you're going to do is just put a flag on it to say some people dispute this film, I think that is a very dangerous precedent.

The Chair: Thank you, Mr. Collins.

We'll go next to Mr. Erskine-Smith.

Go ahead, for five minutes.

Mr. Nathaniel Erskine-Smith: Thanks very much.

You speak to Mr. Zuckerberg often enough, because you're here on his behalf. Remind me why he isn't here today.

Mr. Neil Potts: I'm sorry, sir. I can't see your name.

Mr. Nathaniel Erskine-Smith: It is Mr. Erskine-Smith.

Mr. Neil Potts: Mr. Erskine-Smith, Mr. Zuckerberg and Ms. Sandberg have entrusted us to represent the company here today. We are subject matter experts in these areas, and we're more than happy for the opportunity to be here, but I do want to make—

Mr. Nathaniel Erskine-Smith: He said, “I'm looking forward to discussing these issues with lawmakers around the world” less than two months ago. He just didn't mean these lawmakers. He meant other lawmakers, I'm sure.

I'm going to talk about privacy. In his most recent report, our Privacy Commissioner has said that Facebook's privacy protection framework was “empty”. Then on May 7 before this committee, our Privacy Commissioner said that finding still applies, that it is empty. If Facebook takes privacy seriously, and I heard Mr. Chan say that it does—these aren't my words; these are the Privacy Commissioner's words—why had it “outright rejected, or refused to implement” the Privacy Commissioner's recommendations?

Mr. Kevin Chan: Given that the commissioner has indicated that he will be taking this to Federal Court, we're somewhat limited in what we can say, but what I can share with you is that—

Mr. Nathaniel Erskine-Smith: You're not limited in what you can say at all, Mr. Chan.

Mr. Kevin Chan: I'm going to continue with what I can share with you, which is that we actually have been working quite hard in the last few months to arrive at a resolution and a path forward with the Privacy Commissioner of Canada—

Mr. Nathaniel Erskine-Smith: So you didn't outright reject or refuse to implement the recommendations.

Mr. Kevin Chan: I think we were in a conversation about how we could get to the objectives that we all seek.

● (1115)

Mr. Nathaniel Erskine-Smith: When the Privacy Commissioner wrote those specific words in his specific report, he was incorrect, in your view.

Mr. Kevin Chan: I don't.... If I may, I just want to share a bit more, because I am limited in what I can say—

The Chair: Actually, Mr. Chan....

Mr. Chan, the priority goes to members of the committee, so if you wish to keep speaking, you need to hear.

Mr. Nathaniel Erskine-Smith: Mark Zuckerberg has also said the future is private. Interestingly, of course though, it used to be Facebook privacy policy in 2004 that it did not and would not use cookies to collect private information from any user. That changed in 2007. Initially Facebook gave users the ability to prohibit the collection of their personal information from third parties, and that was again changed.

When Mr. Zuckerberg says the future is private, does he mean the future is going back to our past, when we cared about privacy before profits?

Mr. Kevin Chan: I think we are undertaking a significant effort to reimagine what communications services will look like online. I think there have been a lot of interesting things written, not just by folks at the company but around the world. We do see a trend line such that people are increasingly focused on one-to-one communications. Those are, by definition, private, but what it does raise, sir, in terms of public policy questions is a very interesting balance between privacy and lawful access to information and questions of encryption. These are tight tensions. I think they've been raised previously, including in previous parliaments of Canada, and we look forward to engaging on those questions.

Mr. Nathaniel Erskine-Smith: With regard to engaging on those questions, GDPR has been adopted by the EU. We've recommended, at this committee, that Canada go further initially.

Facebook made $22 billion last year. Alphabet made $30 billion last year. Previously, you've used millions of those dollars to lobby against GDPR. Now you agree that's a standard that ought to be in place or that similar standards ought to be in place.

I'd like a simple yes-or-no answer, Mr. Chan and Mr. Slater.

Mr. Kevin Chan: Yes, we fully support GDPR.

Mr. Nathaniel Erskine-Smith: Mr. Slater.

Mr. Colin McKay (Head, Government Affairs and Public Policy, Google Canada): If you don't mind, Mr. Erskine-Smith, I'll respond as the privacy expert.

Mr. Nathaniel Erskine-Smith: Sure.

Mr. Colin McKay: Yes.

Mr. Nathaniel Erskine-Smith: Mr. McNamee was here and he suggested that perhaps consent shouldn't be the only rule in play and that in certain instances we should simply ban certain practices. He used web tracking.

When was the last time that Google read my emails to target me with ads? How many years ago was it?

Mr. Colin McKay: We stopped using your Gmail content for advertising in 2017. That was specific to you. That information was never shared externally.

Mr. Nathaniel Erskine-Smith: Is that something that we could consider banning so that individuals could never consent to having their emails read to be targeted for advertising? Would you be comfortable with that?

Mr. Kevin Chan: It's certainly the practice that we have now. I hesitate at the word “ban” because there's a broad range of services that might be used in that specific context that make sense.

Mr. Nathaniel Erskine-Smith: The German competition authority, in February of this year, said:

> In view of Facebook’s superior market power, an obligatory tick on the box to agree to the company’s terms of use is not an adequate basis for such intensive data processing. The only choice the user has is...to accept the comprehensive combination of data or to refrain from using the social network. In such a difficult situation the user’s choice cannot be referred to as voluntary consent.

Mr. Chan and Mr. Slater, do you think that privacy is a key consideration in competition and merger decisions, and should competition authorities around the world take privacy issues into account?

Mr. Kevin Chan: I'm sorry. Could you repeat the question just to make sure I understand?

Mr. Nathaniel Erskine-Smith: Do you agree that competition authorities around the world should be looking at privacy—just as they currently look at price—and data collection of our personal information as a key consideration in competition law and when looking at mergers and acquisitions?

Mr. Kevin Chan: That's a very interesting question of public policy. I think, presumably, certain—

Mr. Nathaniel Erskine-Smith: It could just be a yes or no.

Mr. Kevin Chan: These are complex issues, sir, as you can appreciate, and if you would allow me, I would just like to say a few more words with regard to this because it is complicated.

I think it's clear that competition policies and privacy policies are quite different. I suspect that data protection authorities around the world would have very different views about whether or not it is appropriate to pour concepts from other realms into data protection law.

Mr. Nathaniel Erskine-Smith: I'm not suggesting that. I'm suggesting that since we currently protect consumers on price, shouldn't we protect consumers on privacy? We have a German competition authority suggesting that we should do so.

Mr. Kevin Chan: I see. I'm sorry. I understand more clearly what you're saying.

● (1120)

Mr. Nathaniel Erskine-Smith: I did read a quote directly from the German competition authority.

Mr. Kevin Chan: You're absolutely right that data protection... that we should treat privacy as a foundational cornerstone of the digital economy.

Mr. Nathaniel Erskine-Smith: Of competition law....

Mr. Kevin Chan: I believe that these are two very distinct and separate things. It wouldn't just be me. I think that if you talk to competition authorities and data protection authorities, they might very much arrive at similar views.

Mr. Nathaniel Erskine-Smith: That's not the one that I read to you.

Mr. Kevin Chan: We are aware of this. I have spoken to some of my colleagues in Germany with respect to this. Our understanding is that the GDPR needs to, obviously, be enforced and interpreted by data protection authorities in Europe.

The Chair: Thanks.

We need to move on.

We will go next to Monsieur Gourde for five minutes.

[*Translation*]

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

Over the years, the digital platforms you represent have developed very powerful, even overly powerful, tools. You are in the midst of a frantic race for performance. However, it isn't necessarily for the well-being of humanity, but rather for the personal interests of your companies.

Let me make an analogy. You have designed cars that can travel up to 250 kilometres an hour, but you rent them to drivers who travel at that speed in school zones. You have developed tools that have become dangerous, that have become weapons.

As a legislator, I do not accept that you rejected out of hand your responsibility in this regard. These tools belong to you, you have equipped them with functions, but you don't necessarily choose the users. So you rent your tools commercially to people who misuse them.

In the election we'll have in Canada in a few months, will you have the technical ability to immediately stop any fake news, any form of hate advertising or any form of advertising that would undermine our democracy? Will you be able to act very quickly? At the very least, can you stop all advertising during elections in Canada and other countries, if you cannot guarantee us absolute control over the ads that can be placed on your platforms?

We'll start with the representatives from Facebook, then I'd like to hear from Google and Twitter.

Mr. Kevin Chan: Thank you very much, Mr. Gourde.

I'll start by saying that we'll do everything we can to protect the election in October 2019.

As you know, we are working closely with the Conservative Party, the New Democratic Party and the Liberal Party. The other parties should be mentioned, including the Green Party, the People's Party, the Bloc Québécois—

Mr. Jacques Gourde: Excuse me, Mr. Chan, but it isn't about parties. It's about people who will have to make a choice based on the information we will provide to them, not on fake information.

Do you have the ability to quickly stop the spread of fake information or even to stop altogether any advertising that can be placed on your platforms, if you don't have control over it?

Mr. Kevin Chan: Thank you for the question.

Here, in Canada, we have a team that works on each election. We have done this in Ontario, British Columbia, Prince Edward Island, New Brunswick—

Mr. Jacques Gourde: Please don't list all the provinces.

I want to know if you have the ability to stop the spread of any hate advertising or any fake information at any time during the next election.

Mr. Kevin Chan: For the time being, in all the other elections, there have been no problems that we haven't been able to resolve quickly.

Mr. Jacques Gourde: Thank you.

I have the same question for the representatives from Google.

[*English*]

Mr. Derek Slater: Getting this right is absolutely essential. We do invest heavily in efforts to both anticipate and prevent efforts that would interfere with election integrity. That's by making useful information available in search or dealing with actors who might deceive or misrepresent themselves in ads.

Mr. Carlos Monje: Twitter has spent a significant amount of time improving our internal ability to spot this type of disinformation. We've learned from elections around the globe. We've actively engaged with civil society here, most recently in the Alberta elections, and we believe we are very prepared. However, we cannot take our eye off the prize. It's going to be the people who want to manipulate the conversation who will continue to innovate and we will continue to innovate to stay ahead of them.

● (1125)

[*Translation*]

Mr. Jacques Gourde: Based on your answers, I remain doubtful and concerned.

You cars can drive 250 kilometres and hour, but the speed limit on the highway is 100 kilometres an hour. Are you able to reduce the capacity of your tools so that it is fair and equitable for everyone?

What is the point of having such powerful tools if it is to do evil, when a lesser performance could serve the good of humanity?

Mr. Kevin Chan: If I may, I will speak in English to be clearer, since it's my mother tongue.

[*English*]

I just want to say, Mr. Gourde, that's exactly what we're going to do. Next month, as your party and other parties in Canada are aware, we're introducing a very friction-intensive process for anybody who wants to run political ads. We are going to require them to authorize, to demonstrate that they're Canadian. We will need to independently validate the fact that they're Canadian, and then we're going to have to give them a code—or a key, if you will—where they're going to authenticate before they can run an ad.

This is not going to be a thing that happens in an hour. It's not going to be a thing that happens in a day. It's going to be a multi-day process. You have my assurance that we'll be reaching out and working in strict collaboration with all political parties in Canada to take them through this process. Precisely to your point about speed bumps or brakes, I would say this is going to be significant friction in the system, but we think this is the right thing to do in order to get ad transparency right, it's the right thing to do to get regulated political advertising right and it's an important thing to do to guard against foreign interference.

The Chair: Thank you, Monsieur Gourde.

Next up is Mr. Angus.

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

Thank you so much for these presentations. They're very helpful.

Mr. Chan, we know that Mr. Zuckerberg and Ms. Sandberg are very important people. Are they busy today?

Mr. Kevin Chan: I am not aware of their schedules today, but I think that's right. They unfortunately had to send their regrets.

Mr. Charlie Angus: Okay.

I'm trying to get a sense of corporate governance with Facebook. You come from Canadian politics. You worked for the Liberal Party. We're kind of meek and mild here in Canada. I don't ever remember a summons being issued against the head of a corporation. I don't know of anybody who has ever decided to ignore a summons.

Surely to God they have something really pressing to keep them busy. When Mr. Zuckerberg recently spoke, as my colleague pointed out, about his willingness, his desire to talk with legislators. Was that a joke?

This is for Mr. Chan. I'm interested in Mr. Chan because he represents us in Canada.

Mr. Kevin Chan: Well, sir, I have to say that we do desire very much to collaborate with the Parliament of Canada and the Government of Canada. The election that's before us is going to be an important one, and an important one for us to get right at Facebook. We want to ensure a free and fair election. That's why we have done all the things that we have done.

We're complying with Bill C-76. To my knowledge, we may be the only company represented on this panel that is moving forward with an architectured system to do this. We have moved quickly on hate figures and hate organizations in Canada, and we have signed on to the Canada declaration on electoral integrity. I would—

Mr. Charlie Angus: Yes, thank you for that. Sorry, I only have a few minutes.

I appreciate that work. I'm a big fan of Facebook.

Mr. Kevin Chan: Thank you, sir.

Mr. Charlie Angus: I've spoken greatly about the powerful tools it has in the indigenous communities I represent.

My concern is this idea of opt-in, opt-out that Facebook has when it comes to national law. First of all, you ignored a summons by Parliament because Mr. Zuckerberg may be busy. It may be his day off. I don't know.

You were recently found guilty by our regulator in the Cambridge Analytica breach. Our regulator, Mr. Therrien, said:

> Canadians using Facebook are at high risk that their personal information will be used in ways they may not be aware of, for purposes that they did not agree to and which may be contrary to their interests and expectations.
>
> This could result in real harms, including political...surveillance.

What was striking was that Facebook didn't concede that we have jurisdiction over our own citizens. If you're saying you're willing to work with parliamentarians, I don't get this opt-in when it works for Facebook and opt-out when....

Can you give me an example of any company saying that they just don't recognize whether or not we have jurisdiction over our citizens?

● (1130)

Mr. Kevin Chan: Sir, my eyebrows were also raised when I saw those reports, so I did read it carefully and I did talk to legal counsel about it.

My understanding is that this was in reference to the fact that, to our knowledge, based on the available evidence around the world and based on documented evidence, not only in terms of contracts and things like that, but also witnesses who have first-hand accounts, there was no Canadian, or indeed, no non-U.S. user data that was ever transferred to Cambridge Analytica. I believe, if I may—

Mr. Charlie Angus: Okay, but on that point—I only have a short period of time—622,000 Canadians had their data taken. Facebook became aware of it in 2015, and Facebook said nothing until it was exposed internationally because of the Cambridge Analytica breach. That is a breach of Canadian law under PIPEDA.

You know that law, yet to tell Canadian legislators that we had to prove individual harm before Facebook would concede jurisdiction, that to me would be like an international auto company saying, "Yes, there were mass deaths in Brazil; yes, there were mass deaths in the United States; yes, there were mass deaths all over Europe; but since nobody died in a car accident in Canada, we are not going to comply with Canadian law."

How do you get to decide what laws you respect and what laws you figure don't apply to you? Why do you think that?

Mr. Kevin Chan: Mr. Angus, with all due respect, we actually go over and above the law—

Mr. Charlie Angus: No you don't. You don't recognize that we have jurisdiction.

Mr. Kevin Chan: —as the Parliament of Canada knows.

Mr. Charlie Angus: How can you say that to us with a straight face, Mr. Chan? How can you?

Mr. Kevin Chan: Because it is the truth, sir.

Mr. Charlie Angus: So we have to take you to court to get you to recognize that we have jurisdiction to protect our citizens, after you sat on a breach that you knew about for three years and did nothing to tell us about because you didn't want to up-end your business model.

Mr. Kevin Chan: With respect to election integrity, we are going over and above the law—

Mr. Charlie Angus: I'm talking about the privacy rights of Canadians and the breach of our law that you were found guilty of. That's the question.

Mr. Kevin Chan: We can talk about that as well, sir, in the time remaining, if you will permit me.

As I said, we wanted to get to a resolution with the commissioner. He has decided to take us to court, which is of course the framework that's prescribed for him—

Mr. Charlie Angus: He had to take you to court, because you wouldn't concede that we as legislators even have jurisdiction over our own citizens. That's not coming to a resolution. That's like, "Hey, Facebook, is it okay if we come and see, and if it's okay, we'll all work things out?" That is not how law works. Maybe that's how it works for Mr. Zuckerberg, but that's not how it works internationally, which is why we are here. It's because we have international legislators who are frustrated—

Mr. Kevin Chan: We have nothing but the utmost respect for—

Mr. Charlie Angus: —by the lack of respect for international law.

Mr. Kevin Chan: We have the utmost respect for the law in Canada and for legal authority around the world.

The Chair: Thank you.

We'll go on next to Mr. Tong from Singapore.

Mr. Edwin Tong (Senior Minister of State, Ministry of Law and Ministry of Health, Parliament of Singapore): I have limited time, so I would appreciate it if you just focus on my questions and give the answers directly.

We've heard a lot about what you wish to do, who you are engaged with, who you wish to see and how you're going to work on your policies, but let's just see what actually appears and continues to appear on your platforms.

To do that and to save some time, I have put together a little handout that summarizes several cases, which I have no doubt you're familiar with. Just thumb through them quickly. These are all cases that were sensational. They all went viral quickly. They were probably amplified by trolls and bots—fake accounts. They incite fear, they cause disaffection and tensions, and they prey on divisive social fault lines: race, religion, immigration.

One key fact is that they're all false information as well, and all resulted in real world harm: physical injuries, deaths, riots, accentuating divisions and fault lines between religions and races, causing fear.

Just go to the very last page of the handout and look at Sri Lanka, April 2019. The leader of the Easter terrorist bombings in Sri Lanka had posted videos that were on your platforms—Facebook and YouTube—for at least six months prior to the bombing itself. In the videos, he says, "Non-Muslims and people who don't accept Muslims can be killed, along with women and children." Separately, he says, "We can kill women and children with bombs. It is right."

This is clear hate speech, is it not?

Mr. Neil Potts: It is hate speech.

Mr. Edwin Tong: And it's a breach of your own policies, isn't that correct?

Mr. Neil Potts: That would be a breach of our policies. That is correct, sir.

Mr. Edwin Tong: These passages, posted months prior to the Easter bombings, portend what was to come, and it happened, horrifically, in April, in the same fashion as this alleged priest, Mr. Zahran Hashim, said it would—by bombs, killing women and children—on your platforms.

Why? Why was it not removed?

Mr. Neil Potts: Thank you, Mr. Tong.

Just to quickly—

● (1135)

Mr. Edwin Tong: No. Please answer my question. Why was it not removed? You say it's a breach of your own policies. Why was it not removed in September 2018?

Mr. Neil Potts: When we're made aware of that content, we do remove it. If it is not reported or if we have not proactively identified it, then we would not remove it, because honestly we would not know that it exists.

I want to say that our hearts go out to those people in Sri Lanka and everywhere that you've mentioned here in your handout. Intercommunal ethnic violence is a horrific thing. We don't want our platform to be co-opted and used for these activities. In fact, we have taken aggressive action to combat this. We now have more than 30,000 people working in safety and security—

Mr. Edwin Tong: Mr. Potts, I don't need a speech on what you will be doing.

Mr. Neil Potts: I apologize.

Mr. Edwin Tong: How difficult is it to work out that the phrase, "We can kill women and children with bombs. It is right", is hate speech? How difficult is it?

Mr. Neil Potts: That question is not hard, Mr. Tong. The question would be one of identifying the content. If we are not made aware that the content exists, either through a user report or our own proactive measures, then we would not know that this content is on the platform.

Mr. Edwin Tong: So none of the AI, or the technology, or the fact-checkers or the army of people you have scrutinizing your platforms picked this up eight months prior to the event, and you are asking us to trust the processes that you intend to put in place, trust that the AI that you now have will do so in the future.

Mr. Neil Potts: Artificial intelligence is a great lever to help us identify this. It is not perfect. It is not salient where it will get 100% of the activity right, just as humans we will not get 100% of the activity right. I would have to check on this video specifically, but if we were made aware of this video, we would remove it. This is a very straightforward call.

Mr. Edwin Tong: Mr. Potts, if you do some homework and check, local Muslim leaders flagged it to Facebook, and Facebook did not take it down despite being aware of it, despite it being, as you say, a clear breach of your own policies. I'd like to know why.

Mr. Neil Potts: Sir, I would have to see how the content was shared. The way that you have—

Mr. Edwin Tong: You said, Mr. Potts and Mr. Chan, that both of you are content specialists. You are domain specialists. You're here in place of Mr. Zuckerberg and Ms. Sandberg, and you should know. This happened a few months ago, so why was it not taken down despite Facebook being aware of it? Can you explain?

Mr. Neil Potts: I'm trying to explain that I don't know that premise. I'd have to check to make sure that we were actually aware. I do not believe that we were aware of that video at the time.

Mr. Edwin Tong: Let me suggest to you that you didn't remove it because such content is sensational. It incites fear, violence, hatred and conspiracy theories. As Mr. McNamee explained to us earlier, that is what drives eyeballs to your platforms. It's what drives users to your platforms and that is the engine room of your profit mechanism.

Mr. Neil Potts: Mr. Tong, I reject the premise. I reject that wholeheartedly. If we know that something is hate speech, if we know that it is causing violence, we actually move more swiftly.

We had a discussion earlier about misinformation. If we know that misinformation is actually leading to physical harm and violence, we work with trusted partners on the ground, civil society and others, to flag that for us—law enforcement even—and then we will actually remove that content.

Mr. Edwin Tong: Mr. Potts, Facebook was told about this. You can check. Facebook was also told about the problems in Sri Lanka on March 2018 by the Sri Lankan government. It refused to take it down on the basis that it didn't infringe on your own policies. Mr. McNamee says that as a result, governments in Sri Lanka, in Indonesia and in India have had to take proactive action to shut down social media such as Facebook and WhatsApp. Is that how you want this play out?

Can we trust the policies you have in place? Can we trust that what you do and put in place, checks to seek out and remove such content, will actually work?

The Chair: Thank you, Mr. Tong. We'll have to go on to the next question.

We'd like to welcome our delegation from Ireland. They just landed this morning.

Welcome to our committee.

We'll start off our first five minutes with Hildegarde Naughton.

Ms. Hildegarde Naughton (Chair, Joint Committee on Communications, Climate Action and Environment, Houses of the Oireachtas): Thank you, Mr. Chairman. We're delighted to be here this afternoon.

I'll start by listing out my questions for you, and the social media companies can answer afterwards. I have about three questions here. The first is in relation to data protection.

It's very clear that you're all scrambling to figure out how to make privacy rules clear and how to protect users' data. The inception of GDPR has been a sea change in European data protection. The Irish data protection commissioner now has the job of effectively regulating Europe, given the number of social media companies who have their headquarters based in Ireland.

In the 11 months since GDPR came into force, the commissioner has received almost 6,000 complaints. She has said that her concentration on Facebook is because she didn't think that there would be so many significant data breaches by one company, and at one point, there were breaches notified to her under GDPR every fortnight, so she opened a consolidated investigation to look at that. I want to ask Facebook if you can comment on her remarks and why you're having such difficulty protecting users' data.

Also, for this next question, I might ask Google and Facebook to comment. I and my colleague James Lawless and deputy Eamon Ryan met earlier this year with Mark Zuckerberg in Ireland, and he said that he would like to see GDPR rolled out globally. Some of Facebook's biggest markets are in the developing world, such as in Asia and Africa, and out of the top 10 countries, there are only two in the developed world, the United States and the United Kingdom. Some experts are saying that a one-size-fits-all approach won't work with GDPR, because some regions have different interpretations of the importance of data privacy.

I would like to get Google's viewpoint on that—What is your view is in relation to the rollout of GDPR globally? How would that work? Should it be in place globally?—and in relation to the concerns around the different interpretations of data privacy.

Finally, due to the work of our communications committee in the Oireachtas—the Irish parliament—the Irish government is now going to introduce a digital safety commissioner who will have legal takedown powers in relation to harmful communication online. Given that Ireland is the international and European headquarters for many social media companies, do you think that this legislation will effectively see Ireland regulating content for Europe and possibly beyond?

Whoever would like to come in first, please comment on that if you could.

● (1140)

Mr. Kevin Chan: Thank you, ma'am. I want to indicate that Neil and I spent some time with our Irish counterparts, and they have nothing but complimentary things to say about you, so it's nice to meet you.

With respect to the question of breaches that you mention, obviously we are not aware of the specifics that would have been sent to the Irish data protection authority, so I wouldn't be able to comment specifically on that, but I would say our general posture is to be as transparent as we can.

You—and various members at this committee—will probably know that we are quite forward-leaning in terms of publicly revealing where there have been bugs, where there has been some information we have found where we need to pursue investigations, where we're made aware of certain things. That's our commitment to you but also to users around the world, and I think you will continue to hear about these things as we discover them. That is an important posture for us to take, because we do want to do what is right, which is to inform our users but also to inform the public and legislators as much as possible whenever we are made aware of some of these instances.

We want to be very transparent, which is why you will hear more from us. Again, unfortunately, I cannot speak to the specifics that the DPA was referring to.

Ms. Hildegarde Naughton: Google, can I have your comments, please?

Mr. Colin McKay: As we outlined in our opening remarks, we look for international standards that are applicable across a variety of social, cultural and economic frameworks. We look for principle-driven frameworks, particularly in data protection. That has been the history with GDPR as well as the previous OECD principles.

The extension of GDPR beyond its current boundaries is something that is preferable. The question is, how does it adapt to the particular jurisdictions within which it has to operate, considering that the European environment and the history of data protection in Europe is very different from elsewhere in the world, especially the portions of the world, whether Africa or Asia, that you identified?

We're in agreement there. We have been applying the protections that are given to Europeans on a global basis. The question is, what does that look like within a domestic jurisdiction?

On your second question around a digital safety commissioner, I'll turn it over to my colleague Derek.

The Chair: Thank you, Ms. Naughton. We are actually at time, so we have to move on to the next delegate. My apologies. Time is short.

For the next question, we go to the Republic of Germany.

Mr. Jens Zimmermann (Social Democratic Party, Parliament of the Federal Republic of Germany): Thank you very much.

I will also focus first on Facebook. It's great to get to know the Canadian public policy team. I know the German public policy team.

First, I would like to comment on what my colleague from Singapore asked. From my experience in Germany, I have a relatively simple answer. It is simply that many companies, also present today, do not have enough staff to work on all these issues and all these complaints. As has already been mentioned, AI is not always sufficient to work on this. What we've learned in Germany, after the introduction of the NetzDG, is that a massive increase in staff, which is needed to handle complaints, also increases the number of complaints that are handled. I don't know the situation in other countries, but this is definitely an important aspect.

I want to ask about the antitrust ruling in Germany on the question of whether the data from Facebook, WhatsApp and Instagram should be combined without the consent of the users. You are working against that ruling in Germany, so obviously you don't agree, but maybe you can be a bit clearer on your position.

● (1145)

Mr. Kevin Chan: Thank you very much, sir. I understand from one of my colleagues in Canada that she spent some time with you yesterday at a round table. Thank you very much for the invitation.

With respect to the various platforms, our terms of service and our user data policy does underline the fact that we will share data infrastructure between various services, as you know. A big part of it, to be quite frank, is to ensure that we are able to provide some degree of security measures across platforms.

Facebook is a platform where you have your authentic identity. We want to make sure people are who they say they are, but there are lots of good reasons why you will want to have similar kinds of measures on the Instagram platform, for example. There are many instances where—and you would have heard of these in terms of even some of our coordinated inauthentic behaviour takedowns—to be able to do adequate investigations across the system, we actually have to have some ability to understand the provenance of certain content and certain accounts. Having a common infrastructure allows us to very effectively deal with those sorts of challenges.

Mr. Jens Zimmermann: Yes, and it allows you to very effectively aggregate the data, increase the knowledge of the user and also increase the profit. Isn't that the reason behind it?

It would be possible to, again, give all the users the ability to decide on that. That would be very easy, but I think it would also be very costly for you.

Mr. Kevin Chan: I think, sir, what you're touching on in terms of the broader arc of where we're going is correct. We do want to give people more control. We want people to be able to—

Mr. Jens Zimmermann: Okay, but why then are you working against that ruling in Germany?

Mr. Kevin Chan: I think the nub of this is again the question that Mr. Erskine-Smith raised: Where do the limits of competition policy start and end versus the limits of privacy?

Mr. Jens Zimmermann: Okay. Thank you.

I also want to go to Google. You mentioned that you need clear definitions of unlawful speech. I looked into Germany's transparency report and it turns out that of 167,000 complaints in Germany, it was only in 145 cases that your colleagues needed to turn to specialists to determine whether or not this was unlawful speech. Why, then, do you think this is really a problem? Is it really a problem of definition or is it really a problem of handling the number of complaints and the massive amount of hate speech online?

Mr. Derek Slater: That's a very important question. The NetzDG is a complex law, but one of the pieces that is relevant here is that it calls out, I believe, 22 specific statutes that it governs.

Mr. Jens Zimmermann: Actually, the NetzDG basically says that in Germany, you need to comply with German law—full stop.

Mr. Derek Slater: I understand that, and it says, with respect to these 22 statutes, "Here is your turnaround time and your transparency reporting requirements, leading to the data you had." I think part of what is important there is that it refers specifically to clear statutory definitions. These definitions allow us to then act on clear notices in an expeditious manner as set within the framework of the law.

● (1150)

The Chair: Next we will go to the Republic of Estonia.

Go ahead, for five minutes.

Ms. Keit Pentus-Rosimannus (Vice-Chairwoman, Reform Party, Parliament of the Republic of Estonia (Riigikogu)): Thank you.

I come from Europe, from Estonia. It is true that, two days after the European election, one can say that you actually have made progress in removing the fake accounts, but it is also true that those fake accounts should not have been there in the first place.

My first question is the following: What kinds of changes are you planning to use to identify your users in the beginning?

Mr. Kevin Chan: Thank you for that. I think we are cautiously pleased with the results in terms of the way the platform has performed in Europe. However, with respect to fake accounts, I would say—and I think my colleague Neil has mentioned—that this is a bit of an arms race with our adversaries, with bad actors trying to put inauthentic accounts and content onto the platform.

I think we want to constantly get better and to constantly evolve—

Ms. Keit Pentus-Rosimannus: How do you improve the identification process in the first place?

Mr. Kevin Chan: One of the things I can share with you, again in terms of the political advertising piece that we are trying to do, is that we are trying to get a very good certainty as to the identity of the individuals when they run an ad.

In Canada, as I mentioned earlier, we will do this and it will be not without pain. For political advertisers in Canada, it's very much that we will need to get some kind of ID from you. We will need to independently verify that ID, and then we're going to send you some kind of key—a digital key if you will—that you're going to have to use to authenticate yourself before you can even run a political ad.

This is a very costly and significant investment. It is also not without friction. I personally worry that there will be instances where people want to run an ad, don't know about this requirement and then find it's going to take many days to do.

I also worry that there may be false positives, but I think this is the right thing to do to protect elections around the world and here in Canada in October. We're prepared to put in the time, the investment and potentially some of the friction to get it right.

Ms. Keit Pentus-Rosimannus: All right. Thank you.

My second question will be about fake news or fake videos. What is your policy towards fake news, for example, deepfake? Will they be removed or will they just be marked as deepfake videos?

Mr. Derek Slater: The issue of deepfakes.... Thanks for that question. It's a really important emerging issue. We have clear guidelines today about what content should be removed. If a deepfake were to fall under those guidelines, we would certainly remove it.

We also understand this needs further research. We've been working actively with civil society and academics on that.

Ms. Keit Pentus-Rosimannus: What about Facebook?

Mr. Neil Potts: Thank you.

We are also investigating and doing research on this policy, to make sure we are in the right place. Currently, we would identify it as being fake and then inform our users, but we constantly—

Ms. Keit Pentus-Rosimannus: The deepfake will stay on.

Mr. Neil Potts: We constantly iterate our policies, and we may update those policies in the future, as they evolve. We are working with research agencies and people on the ground to understand how these videos could manifest. As I mentioned before, if these videos, or any type of misinformation, led to real world harm—or off-line harm, I should say—we would remove that content.

Ms. Keit Pentus-Rosimannus: What about Twitter?

Mr. Carlos Monje: We also share concerns about deepfakes. If we see the use of deepfakes to spread misinformation in a way that violates our rules, we'll take down that content.

Ms. Keit Pentus-Rosimannus: My last question will come back to what Mr. Collins asked in the beginning, about the fake video of Nancy Pelosi. Let's say a similar video were to appear, only the person there was Mr. Zuckerberg. Would that video be taken down, or just marked as a fake one?

Voices: Oh, oh!

Mr. Neil Potts: I'm sorry, the laughter.... I didn't hear the name?

Ms. Keit Pentus-Rosimannus: Sorry for the loud laughter. If a video similar to what has been airing, picturing Nancy Pelosi, appeared with Mark Zuckerberg, would you remove that fake video, or would you just mark it as fake news?

Mr. Neil Potts: If it was the same video, inserting Mr. Zuckerberg for Speaker Pelosi, it would get the same treatment.

The Chair: Thank you.

I want to give a brief explanation of what's going on behind me. Your chairs have elected to have a working lunch. Feel free to come up and grab something to eat, and we'll continue with testimony all the way through our lunch.

Next up, we have Mexico. Go ahead for five minutes.

● (1155)

Hon. Antares Guadalupe Vázquez Alatorre (Senator): [*Delegate spoke in Spanish, interpreted as follows:]*

Thank you. I'm going to speak in Spanish.

I have several questions. In the case of Google, what do you do to protect people's privacy? I know many cases of sexting videos that are still there in the world, and when the victims of those videos go specifically to your office in Mexico—and I have known about several cases—the Google office tells them to go to the United States to complain. These are videos that are violently attacking somebody and cannot be downloaded. What do you do in those cases?

Mr. Derek Slater: I'm not familiar with the particular cases you're talking about, but we do have strict guidelines about things like incitement to violence, or invasion of privacy and the like. If notified, and if we become aware of it, we would take action, if it's in violation of those guidelines. I'm not familiar with the specific cases, but would be happy to inquire further.

Hon. Antares Guadalupe Vázquez Alatorre: [*Delegate spoke in Spanish, interpreted as follows:*]

I have information about very specific cases, but we don't know who to turn to in Mexico because they reject people. We hope you will take over this case, because the people have to wait for years to withdraw those things.

I'd like to ask Twitter about the creation of trends with robots. It's very common in Mexico. Every day, we have trends created with robots—the so-called bot farms. I don't know what the policy is at Twitter, because you seem to allow the artificial trends, or hashtags, when they are harming somebody. Why don't you allow trends to happen organically? I agree with having trends, things becoming viral and respecting freedom of expression, but why are robots allowed? If anybody can detect them, why is it Twitter cannot?

Mr. Carlos Monje: Trends measure the conversation in real time and try to distinguish conversations that are always having a high level of engagement, English Premier League or the Mexican election writ large. What trends are trying to identify is acceleration above the normal. When that happens organically, like you mentioned, it has a different pattern from when it happens augmented by bots.

Since 2014, which for us is a lifetime, we've had the ability to protect trends from that kind of inorganic automated activity. Kevin mentioned an arms race. I think that's a good term for the battle against malicious automation. Right now we're challenging 450 million accounts a year for being inauthentic, and our tools are very subtle, very creative. They look at signals like instant retweets or activity that's so fast that it's impossible to be human.

Despite that, 75% is what ultimately gets kicked off the service, so 25% of the people who we thought were acting in an inauthentic way were able to pass the challenge. We are over-indexing to try to stop this inauthentic activity. This is a place where there is no delta between the societal values of trusting online activity and our imperatives as a company, which is that we want people when they come to Twitter to believe in what they see, to know that they are not getting messed about with Russian bots or whatever, so we work very hard to get this right and we're continuing to make improvements on a weekly basis.

Hon. Antares Guadalupe Vázquez Alatorre: [*Delegate spoke in Spanish, interpreted as follows:*] But this happens normally every day, not during elections. It's happening every time that a trend is inflated with bots. There's been no adequate response to this. There are things that are aggressive.

This is for Twitter and for Facebook. When a user reports something that has been published, very commonly they report that they are not breaching their policy but they are aggressive against the person. They tell us that it's not breaching the policy, but it's somebody who is lying, who is attacking, and the person feels vulnerable. Many a time nothing happens because it's not breaching your policies.

Also, with this thing about the authentication, when the accounts are authenticated with blue arrows, even the other accounts can be blocked. Some people say identify yourself and they block all the accounts. Meanwhile, there are thousands of fake accounts and nothing happens, even if they are reported. There are users who are constantly reporting these fake accounts. Why do you have a different policy?

● (1200)

The Chair: Give a short answer, please.

Mr. Carlos Monje: We are working to adjust our policies. We have things that are against our rules and we have things that aren't against our rules but that people don't like. We call it, internally, the gap. What we've been doing and what our teams have been doing is trying to break those issues down, portion by portion, and understand where the expectations of our users don't match the experience they're getting.

Our approach is, again, very consistent. We want people to feel comfortable, to feel safe to come online. We also don't want to squelch public expression, and these are issues that we care about deeply and take very personally.

The Chair: Thank you.

Next up, we'll go to the Kingdom of Morocco for five minutes.

[*Translation*]

Mr. Mohammed Ouzzine (Deputy Speaker, Committee of Education and Culture and Communication, House of Representatives of the Kingdom of Morocco): Thank you, Mr. Chair.

I would also like to thank the kind team doing us the honour of being here today: Kevin Chan, Derek Slater, Neil Potts, Carlos Moje and Michele Austin. We would have liked Mark Zuckerberg to be with us, but he let us down. We hope he will return some other time.

I have been very attentive to two proposals from Mr. Chan. I would like to make a linguistic clarification for interpreters: when I use the word "*proposition*", in English, it refers to the term "proposition", and not "proposal".

In presenting the issues raised by his company, Mr. Chan said that it was not just Facebook's responsibility to resolve them. We fully agree on this point.

And then, again on these issues, he added that society must be protected from the consequences. Of course, these platforms have social advantages. However, today we are talking about the social unrest they cause; this is what challenges us more than ever.

Facebook, Twitter and YouTube were initially intended to be a digital evolution, but it has turned into a digital revolution. Indeed, it has led to a revolution in systems, a revolution against systems, a revolution in behaviour, and even a revolution in our perception of the world.

It is true that today, artificial intelligence depends on the massive accumulation of personal data. However, this accumulation puts other fundamental rights at risk, as it is based on data that can be distorted.

Beyond the commercial and profit aspect, wouldn't it be opportune for you today to try a moral leap, or even a moral revolution? After allowing this dazzling success, why not now focus much more on people than on the algorithm, provided that you impose strict restrictions beforehand, in order to promote accountability and transparency?

We sometimes wonders if you are as interested when misinformation or hate speech occurs in countries other than China or in places other than Europe or North America, among others.

It isn't always easy to explain why young people, or even children, can upload staged videos that contain obscene scenes, insulting comments or swear words. We find this unacceptable. Sometimes, this is found to deviate from the purpose of these tools, the common rule and the accepted social norm.

We aren't here to judge you or to conduct your trial, but much more to implore you to take our remarks into consideration.

Thank you.

● (1205)

Mr. Kevin Chan: Thank you very much, Mr. Ouzzine.

Again, please allow me to answer in English. It isn't because I can't answer your question in French, but I think I'll be clearer in English.

[*English*]

I'm happy to take the first question with respect to what you were talking about—humans versus machines or humans versus algorithms. I think the honest truth on that is that we need both, because we have a huge amount of scale, obviously. There are over two billion people on the platform, so in order to get at some of the concerns that members here have raised, we do need to have automated systems that can proactively find some of these things.

I think to go back to Mr. Collins's first question, it is also equally important that we have humans that are part of this, because context is ultimately going to help inform whether or not this is malicious, so context is super important.

If I may say so, sir, on the human questions, I do think you are hitting on something very important, and I had mentioned it a bit earlier. There is this need, I think, for companies such as Facebook not to make all of these kinds of decisions. We understand that. I think people want more transparency and they want to have a degree of understanding as to why decisions were arrived at in the way they were in terms of what stays up and what goes down.

I can tell you that in the last few months, including in Canada, we have embarked on global consultation with experts around the world to get input on how to create an external appeals board at Facebook, which would be independent of Facebook and would make decisions on these very difficult content questions. We think there is—at least as our current thinking in terms of what we put out there—this question of whether they should be publicly binding on Facebook. That is sort of the way we have imagined it and we are receiving input and we will continue to consult with experts. Our commitment is to get this done by 2019.

Certainly, on our platform, we understand that this is challenging. We want a combination of humans and algorithms, if you will, but we also understand that people will have better confidence in the decisions if there is a final board of appeal, and we're going to build that by 2019.

Of course, we're all here today to discuss the broader question of regulatory frameworks that should apply to all services online. There, once again obviously, the human piece of it will be incredibly important. So thank you, sir, for raising that, because that's the nub, I think, of what we're trying to get at—the right balance and the right framework per platform but also across all services online.

The Chair: Thank you, Mr. Chan.

Next up, we will go to Ecuador for five minutes.

Ms. Elizabeth Cabezas (President, National Assembly of the Republic of Ecuador): [*Delegate spoke in Spanish, interpreted as follows:*]

Thank you very much.

I want to talk about some of the concerns that have already been mentioned at this meeting, and also express great concern regarding tweets and Twitter, on which there is a proliferation in the creation of false accounts that are not detected. They definitely remain active for a very long time on social networks and generate, in most cases, messages and trends that are negative and against different groups, both political and those that are linked to businesses or unions in many different areas.

I don't know what mechanisms you have decided to choose to verify the creation of these, because these are accounts that have to do with troll centres or troll farms, which in the case of Ecuador have really cropped up very frequently and which continue to. They have been spreading messages on a massive scale, malicious messages that counteract real information and true information and really twist the points of view.

More than continuing to mention the issues that have already been mentioned, I would urge you to think about fact-checking mechanisms that can detect these accounts in a timely manner, because definitely you do not do it quickly enough or as quickly as is necessary. This allows damaging messages to proliferate and generate different thoughts, and they distort the truth about a lot of subjects.

I don't know what the options are, in practice, or what you're going to be doing in practice to avoid this or prevent this, and to prevent the existence of these troll centres and the creation of accounts that are false, of which there are many.

● (1210)

Mr. Carlos Monje: Thank you. That is exactly the right question to ask, and one that we work on every day.

I'll just note that our ability to identify, disrupt and stop malicious automation improves every day. We are now catching—I misspoke earlier—425 million accounts, which we challenged in 2018.

Number one is stopping the coordinated bad activity that we see on the platform. Number two is working to raise credible voices—journalists, politicians, experts and civil society. Across Latin America we work with civil society, especially in the context of elections, to understand when major events are happening, to be able to focus our enforcement efforts on those events, and to be able to give people more context about people they don't understand.

I'll give you one example because I know time is short. If you go onto Twitter now, you can see the source of the tweet, meaning, whether it is coming from an iPhone, an Android device, or from TweetDeck or Hootsuite, or the other ways that people coordinate their Twitter activities.

The last piece of information or the way to think about this is transparency. We believe our approach is to quietly do our work to keep the health of the platform strong. When we find particularly state-sponsored information operations, we capture that information and put it out into the public domain. We have an extremely transparent public API that anybody can reach. We learn and get better because of the work that researchers have undertaken and that governments have undertaken to delve into that dataset.

It is an incredibly challenging issue, I think. One of the things you mentioned is that it's easy for us to identify instantaneous retweets and things that are automated like that. It is harder to understand when people are paid to tweet, or what we saw in the Venezuelan context with troll prompts, those kinds of things.

We will continue to invest in research and invest in our trolling to get better.

The Chair: We'll move on to the last on our list and then we'll start the sequence all over again.

To Saint Lucia, please go ahead for five minutes.

Mr. Andy Daniel (Speaker, House of Assembly of Saint Lucia): Thank you, Mr. Co-chair.

My questions are to Neil Potts, Global Policy Director. I have two questions.

The first one is that I would like to understand and to know from him and from Facebook, generally, whether or not they understand the principle of “equal arms of government”. It would appear, based on what he said earlier in his opening remarks, that he is prepared and he is willing to speak to us here, and Mr. Zuckerberg will speak to the governments. It shows a.... I do not understand...not realizing the very significant role that we play as parliamentarians in this situation.

My next question is with reference to Speaker Nancy Pelosi's video, as well as to statements made by him with reference to Sri Lanka. He said that the videos would only be taken down if there were physical violence.

Let me just make a statement here. The Prime Minister of Saint Lucia's Facebook accounts have been, whether you want to say “hacked” or “replicated”, and he is now struggling out there to try to inform persons that this is a fake video or a fake account. Why should this be? If it is highlighted as fake, it is fake and it should not be....

Let me read something out of the fake...and here is what it is saying, referring to a grant. I quote:

> It's a United Nation grant money for those who need assistance with paying for bills, starting a new project, building homes, school sponsorship, starting a new business and completing an existing ones.
>
> the United nation democratic funds and human service are helping the youth, old, retired and also the disable in the society....

When you put a statement out there like this, this is violence against a certain vulnerable section of our society. It must be taken down. You can't wait until there is physical violence. It's not only physical violence that's violence. If that is the case, then there is no need for abuse when it is gender relations, or otherwise. Violence is violence, whether it is mental or physical.

That is my question to you, sir. Shouldn't these videos, these pages, be taken down right away once it is flagged as fake?

● (1215)

Mr. Neil Potts: If it is the case that someone is misrepresenting a member of government, we would remove that if it is flagged. I will follow up with you after this hearing and make sure that we have that information and get it back to the team so that we can act swiftly.

Maybe perhaps to address a few of the other conversations here, there's been this kind of running theme that Mr. Zuckerberg and Ms. Sandberg are not here because they are eschewing their duty in some way. They have mandated and authorized Mr. Chan and me to appear before this committee to work with you all. We want to do that in a very co-operative way. They understand their responsibility. They understand the idea of coequal branches of government, whether that's the legislative branch, the executive branch or the judicial branch. They understand those concepts and they are willing to work. We happen to be here now to work on—

The Chair: With respect, Mr. Potts, I'm going to step in here.

With respect, it is not your decision to select whether you're going to come or not. The committee has asked Mr. Zuckerberg and Ms. Sandberg to come, plain and simple, to appear before our international grand committee. We represent 400 million people, so when we ask those two individuals to come, that's exactly what we expect. It shows a little bit of distain from Mark Zuckerberg and Ms. Sandberg to simply choose not to come. It just shows there's a lack of an understanding about what we do, as legislators, as the member from Saint Lucia mentioned. The term “blowing us off”, I think, can be brought up again, but it needs to be stated that they were invited to appear and they were expected to appear and they're choosing not to. To use you two individuals in their stead is simply not acceptable.

I'll go back to Mr. Daniel from Saint Lucia.

Mr. Neil Potts: Thank you, Mr. Zimmer. I want to be clear. I'm not familiar with the procedures of Canadian Parliament and what requires appearance. I respect that, but I do want to get on record that they are committed to working with government, as well as being responsible toward these issues.

Additionally—

The Chair: I would argue, Mr. Potts, if that were the case, they would be seated in those two chairs right there.

Continue on.

Mr. Neil Potts: Additionally, just to address another question that I think is permeating, about how we go about removing content and identifying it, we do remove content for a number of various abuse types. It's not just violence. In that specific case, where we're talking about misinformation, the appearance of some of these tropes that appeared in Sri Lanka and other countries, we removed that on the cause that it would lead to violence. But we have policies that cover things like hate speech, where violence may not be imminent. We have things like personal identifiable information, bullying, which we take very seriously, that may not lead directly to violence but we do enforce those policies directly and we try to enforce them as swiftly as possible.

We now have 30,000 people globally working on these issues. There was a comment earlier about having people with the right amount of context to really weigh in. For all the countries that are represented here, I just want to say that, within that 30,000 people, we have 15,000 content moderators who speak more than 50 languages. They work 24 hours a day, seven days a week. Some of them are located in countries that are here before us today. We take that very seriously.

Additionally, we do have a commitment to working with our partners—government, civil society and academics—so that we are arriving at the answers that we think are correct on these issues. I think we all recognize that these are very complex issues to get right. Everyone here, I think, shares the idea of ensuring the safety of our community, all of whom are your constituents. I think we share those same goals. It's just making sure that we are transparent in our discussion and that we come to a place where we can agree on the best steps forward. Thank you.

The Chair: Thank you.

It was just brought to my attention, too, the inconsistency in your testimony, Mr. Potts.

On one hand, Mr. Collins had asked you about the Pelosi video, which you're not going to pull down. Then within 30 minutes or within an hour you just answered the member from Saint Lucia that it would come down immediately. I just would like you to be completely aware that it's expected that you completely tell the truth to this committee at this time and not to be inconsistent in your testimony.

● (1220)

Mr. Neil Potts: Mr. Zimmer, if I was inconsistent, I apologize, but I don't believe that I answered the question differently. If I had a transcript, obviously I would flag where my discrepancy was and correct it immediately.

Again, on misinformation that is not leading to immediate harm, we take an approach to reduce that information, inform users that it is perhaps false, as well as remove inauthentic accounts. If someone is being inauthentic, representing that they are someone else, we would remove that. Authenticity is core to our principles, authentic individuals on our platform. That's why we require real names.

The question that I believe Mr. Collins was asking was about the video, the video itself. It's not that the user was inauthentic in his sharing of the video. The user is a real person or there's a real person behind the page. It's not a troll account or a bot or something like that. We would remove that.

If I misspoke, I apologize, but I want to be clear that I don't think my—

The Chair: I don't think it's any clearer to any of us in the room, but I'll move on to the next person.

We'll go to Mr. Baylis, for five minutes.

Mr. Frank Baylis (Pierrefonds—Dollard, Lib.): Thank you. I'll start off with Mr. Slater.

A couple of weeks ago, we had another one of your gentlemen in, telling us that Google would not comply with Bill C-76, our new election campaign law. I asked, “Why not?” He said, “Well, we can't get the programming done in six months' time.”

I pointed out that Facebook can, and he said, “Well, our systems are more difficult and it's more complicated.”

He said, “We can't do it in six months”, so I asked him, “Okay, how much time do you need? When can you get it done?” He said he didn't know.

Can you explain that?

Mr. Derek Slater: They've given you extensive information on this front, but just to add a bit, yes, we are a different service, and while we knew regrettably that we would not be in a position to offer election advertising in this time, we would look to it in the future.

Mr. Frank Baylis: If you can say you can't do it in six months' time but you don't know how long it will take, how do you know you can't do it in six months, when Facebook can do it in six months?

Mr. Derek Slater: We are very different services with different features of various types.

Mr. Frank Baylis: How do you not know how long it will take?

Mr. Derek Slater: In part, it's because things continue to change over time. It's a rapidly evolving space, both legally and in terms of our services. Therefore, in terms of exactly when it will be ready, we wouldn't want to put—

Mr. Frank Baylis: You know you can't do it in six months.

Mr. Derek Slater: Yes.

Mr. Frank Baylis: However, you don't know how long it would take.

Mr. Derek Slater: Correct.

Mr. Frank Baylis: I was worried about that, so I asked, “What happens, then, if someone puts up an ad that they're not allowed to?” He said not to worry about that, and do you know why? He said they'll find it instantaneously; they can pick it off.

I asked, “How do you do that?” and he said they have this artificial intelligence and they have a team of people.

Now it says you can find the ad instantaneously, but our law says once you have the ad, you have to put it up. You have 24 hours to put it in a database. That, you can't do.

Can you explain that to me? How is it possible that you have all this technology, you can identify any ad from any platform instantaneously, but you can't have your programmers put it up in 24 hours on a database, and it will take more than six months to do so?

Mr. Derek Slater: If I understand the question correctly, it is simpler to take a more conservative approach, an approach that is more broadly restrictive than one that says, yes, we're going to validate that this is an election ad operating under the law, and so on and so forth.

Mr. Frank Baylis: You're already making a decision. You're validating it because you're blocking it. He told me that. You're doing that.

Mr. Derek Slater: Yes, we may be blocking it for a variety of reasons if it violates our policies.

Mr. Frank Baylis: No, not your policies; he said “political ads”. My question was very specific.

You can stop it, but you can't put it on a database. I want to understand the difference.

Mr. Derek Slater: There is a big difference between saying we're going to take, in general, a conservative approach here and saying, on the other hand, “I'm going to say clearly this is a legitimate election ad”, taking that further step.

Mr. Frank Baylis: Once you see that it's an ad, you're not letting it go up. You're blocking it. You can instantaneously decide it's an ad, but once you've decided it's an ad, it's too much work to program it to put it in a database. That's what our law asks: Just put it in a database.

You're saying, “That, we can't do.”

Mr. Derek Slater: The needs of implementing the law in the specific way it was written were prohibitive for us in this period of time to get it right, and if we're going to have election ads in the country, we absolutely need to and want to get it right.

That was the decision we had to make here, regrettably, but we look forward to working on it in the future.

Mr. Frank Baylis: You could decide that you couldn't do it in six months' time, even though someone else could do it, and you decided you can instantaneously capture any ad from anywhere at any time, but you don't have the technological capability at Google to put it in a database within 24 hours. You just don't have that capability to program that in six months.

Mr. Derek Slater: We do not have the capability at this time to comply in fullness with that law.

● (1225)

Mr. Frank Baylis: You don't have the capability. Are you serious when you say that?

Are you serious when you say that you can identify any ad from any platform anywhere, but you can't get your programmers to put it in a database? It will take too long for you to program moving it from being identified to just putting it in a database.

Mr. Derek Slater: I can't speak to everybody's services everywhere. To be clear, we use machines and people to monitor ads that are submitted through our systems to make sure they are in compliance with our rules.

In terms of the additional obligations, no, we were not able to meet them in this case.

Mr. Frank Baylis: Okay. I have another question for Google and Facebook, a simple question.

I don't like your terms of use. What can I do about it?

Mr. Kevin Chan: Sir, if you could explain to me, perhaps give me a bit more colour about what you don't like about it....

Mr. Frank Baylis: I don't like being spied on.

Mr. Kevin Chan: Oh, well, we don't do that, sir.

Mr. Frank Baylis: You collect data on me that I don't want you to collect.

Mr. Kevin Chan: As you know, I do spend a lot of time on digital literacy space. What is appropriate is for people to not put as much as they do not wish to put on the service.

Sir, if I may, to get to a different point on this, we are, as you know I think, going to be releasing a very different type of product experience in the next little while, where you're going to be able to remove not only information we have that you've put onto the service, but you're going to be able to remove also information that would have been on the service because of integrations with other services across the Internet. We are going to give you that functionality, so again, to the extent that is not desirable for you, we do want to give you that control.

The Chair: Thank you, Mr. Baylis. Unfortunately, we have to move on.

Next up for five minutes is Mr. Kent.

Hon. Peter Kent: Thank you, Chair.

This is a question for Mr. Chan.

If a Canadian employer came to Facebook and wanted to place an employment ad microtargeting by age and sex and excluding other demographic groups, would Facebook accept that ad?

Mr. Kevin Chan: Sir, thank you for the question. Again, I want to also thank you for extending an invitation to us to be part of your recent round table in Oshawa. It was greatly appreciated.

That would be a violation of our policies, so it would not be accepted.

We have a couple of things and I think I understand what you're getting at—

Hon. Peter Kent: If I can, because time is short.... Would it shock you to learn that we in the official opposition of Parliament have received an answer to an Order Paper question today that says that several Government of Canada departments have placed ads with exactly those microtargeted conditions and that your company is named a number of times.

Mr. Kevin Chan: Sir, that is, as you know, through the incredibly thorough reporting of Elizabeth Thompson from the CBC, also out in the public domain, because I read it there first.

You should know that this is a violation of our policy, sir. We have actually moved quite aggressively in the last little while to remove a whole bunch of different targeting abilities for these types of ads. We have also—for housing, employment and credit ads, to be clear—required all advertisers on a go-forward basis to certify that they are not running housing and credit and employment ads.

Hon. Peter Kent: Have you informed the Government of Canada that this sort of microtargeting practice by the Liberal Government of Canada will no longer be accepted? Just give a yes or no.

Mr. Kevin Chan: We have sent out emails to all admins telling them that they cannot do this.

Hon. Peter Kent: Coming back to Mr. Collins' original question about the manipulated, sexist, politically hostile video that has been allowed to stay on your Facebook platform, I understand that after *The Washington Post* contacted Facebook, a statement was issued saying, "We don't have a policy...that the info you post on Facebook must be true".

From your earlier answers, it would seem that Facebook is refusing to remove this politically hostile video, claiming a sort of perverted defence claim of free speech, and that in the 24 hours after *The Washington Post* made that notification to you, they report that there was a viewership, on a single Facebook page, of more than 2.5 million views and that it was multiplied many times on other Facebook pages.

If that were to happen in the Canadian election—a similar video of a Canadian politician, perhaps the leader of one or another of the parties were to be posted and manipulated in the same way to give the impression of mental incapacity or intoxication—would Facebook remove that video, or would you do what you maintained in your answers to Mr. Collins, simply say that it's not true, despite those who would continue to exploit the falseness of the video?

● (1230)

Mr. Kevin Chan: Sir, just leaving aside the specific video in question that is originating from the United States, we have been at this and I have been at this personally for the last two-plus years, trying to find ways to better secure the platform for the upcoming election.

I can tell you that when we receive requests from various sectors and people and parties, 99% of the time when we find something that has been reported to us, we actually go beyond what the content is. We're not looking for the content. We're looking for the behaviour.

Hon. Peter Kent: But would you take it down?

Mr. Kevin Chan: If it originates from a fake account or if it's deemed to be spam, or if it is a violation otherwise of a community's standards, absolutely we would.

I can assure you that in almost every instance that I—

Hon. Peter Kent: But it is false. It's not the truth. Does Facebook still defend the concept that it doesn't have to be truthful to be on your platform?

Mr. Kevin Chan: Sir, I understand what you're getting at. I think that, if you'll permit me, the way I would like to maybe talk about it a bit is—

Hon. Peter Kent: Yes or no would work.

Mr. Kevin Chan: That's why we're here. We would welcome basic—

Hon. Peter Kent: So is this a learning experience for you?

Voices: Oh, oh!

Mr. Kevin Chan: Mr. Kent....

Hon. Peter Kent: I ask that with respect and civility.

Mr. Kevin Chan: We would welcome basic standards that lawmakers can impose on the platform about what should go up and what should come down. If lawmakers, in their wisdom, want to draw the line somewhere north or south of censorship, we would, obviously, oblige the local law.

Hon. Peter Kent: Perhaps I will close by commenting.

Chris Hughes, a disillusioned co-founder of Facebook who has become something of a whistle-blower again for some, says that "Facebook isn't afraid of a few more rules. [Facebook is] afraid of an antitrust case".

Are you aware that, in democracies around the world, you are coming closer and closer to facing antitrust action?

Mr. Kevin Chan: I am aware of multiple questions with respect to regulation around the world, yes, sir.

Hon. Peter Kent: Thank you.

The Chair: Thank you, Mr. Kent.

Just so that you're aware, I want to remind you all about the sequence of questioning. We're going one question per delegation first, through the countries. You can see how the pattern has been established. Then there are going to be different rounds until all the members have had a chance to ask a question. For example, the next member in the delegation would ask the next question, etc.

Right now we have the second member of the delegation for the U.K., Mr. Lucas. He will be asking the next five-minute question, or maybe Jo Stevens.

Prepare yourself for that. I might look to different countries. If you have a second delegate, he or she will be given the opportunity to ask a question as well.

Go ahead, Ms. Stevens, for five minutes.

Ms. Jo Stevens (Member, Digital, Culture, Media and Sport Committee, United Kingdom House of Commons): Thank you, Mr. Chair.

Mr. Potts and Mr. Chan, I want to say thank you for coming today, but my colleagues and I from the U.K. Parliament wanted to ask Mark Zuckerberg our questions. He wouldn't come to answer our questions in London at our Parliament, so we have come across the Atlantic to make it easier for him. We can only conclude that he's frightened of scrutiny. For the avoidance of doubt, I am sick to death of sitting through hours of platitudes from Facebook and avoidance tactics with regard to answering questions. I want the boss here to take responsibility, so please take that message back to Mr. Zuckerberg.

I'd like to ask the Google representatives a question.

In any other sector, your company's monopolistic position would have been dismantled by now. What are you doing at the moment to prepare yourselves for that eventuality?

Mr. Colin McKay: I think we're working very hard to demonstrate to our users and to regulators that we bring value to the marketplace and to our users. They have a clear understanding—whether they're using our maps in signed-in or incognito mode, whether they're using Gmail, or whether they're using our infrastructure services—that there is a value for them and that we're playing a positive role in the marketplace not only by providing value for them in terms of computing services, but also by providing products and services that help businesses grow around the world.

We think regulators have a right and, certainly, a duty to scrutinize our business and to examine it within the framework that they have that's been set up through their local jurisdictions. We will participate in that process and try to explain how we think we're providing that value when we're meeting the obligations of the regulations as they have interpreted them.

● (1235)

Ms. Jo Stevens: However, you're not taking any steps at the moment to prepare yourself for cases.

Mr. Colin McKay: At the moment, we're focusing on providing services that both fulfill and anticipate the needs of our users.

Mr. Ian Lucas: Perhaps I could ask about a specific hearing that Facebook gave evidence at in February 2018. When we asked Facebook about Cambridge Analytica in Washington, we were not informed of the data incident involving Cambridge Analytica and Aleksandr Kogan.

Mr. Potts, with regard to transparency, which you raised, why were we not informed about the Cambridge Analytica incident, which we specifically raised on that day?

Mr. Neil Potts: Thank you, Mr. Lucas.

I'm sorry, but I'm not quite clear on what happened during that hearing. I can try to find out exactly what was presented and what evidence was given, but I, unfortunately, don't recall what was given.

Mr. Ian Lucas: It's a matter of public record. The reason we want Mark Zuckerberg here is that we want clear evidence from Facebook executives about specific questions that we've asked.

Mr. Chan, can you answer the question for me?

Mr. Kevin Chan: Sir, I'm afraid that I don't want to speak out of turn, but we're not familiar with the transcript of what happened in, I think you said, February 2018. Certainly we would undertake to find out.

Mr. Ian Lucas: I can tell you exactly what happened. I could read the position. We raised the issue of Cambridge Analytica, the data incident and the issue related to Cambridge Analytica. We were not told that there had been a data incident involving Aleksandr Kogan, which came out subsequently in the newspapers within two months. You're aware of that incident, I assume.

Mr. Neil Potts: We are aware of Cambridge Analytica. Again, we don't know, I guess, what attestations were made.

Mr. Ian Lucas: Did you regard that incident as a serious matter, the Cambridge Analytica incident?

Mr. Neil Potts: Yes, Mr. Lucas.

Mr. Ian Lucas: Do you know what steps were taken within Facebook when the Cambridge Analytica incident involving Aleksandr Kogan...? What steps were taken? Do you know?

Mr. Kevin Chan: If I understand your question, since 2014 we have significantly reduced—

Mr. Ian Lucas: I asked you a specific question. What steps were taken within Facebook when you became aware of the Cambridge Analytica incident? I'm choosing my words very carefully, more sympathetically than most would. Some people would call this a data breach, but on the incident involving Aleksandr Kogan, what steps were taken by Facebook?

Mr. Kevin Chan: Specifically with Aleksandr Kogan's app, that app is banned from the platform, sir.

Mr. Ian Lucas: Who made that decision?

Mr. Kevin Chan: The company.... I couldn't tell you. If you were looking for a specific individual, I really couldn't tell you, but the company—

Mr. Ian Lucas: The specific individual I'd like to be asking this question of is Mark Zuckerberg because I want to know if he knew about this incident then. Did he know?

I've asked Mike Schroepfer this question and he told me he'd get back to me. That was last summer. Did Mark Zuckerberg know about that breach in 2015?

Mr. Kevin Chan: Sir, we are very happy to get you an answer to that. To the extent that you haven't had it, which seems to be what you are saying, we apologize. We obviously want to always co-operate with questioning—

Mr. Ian Lucas: Can I just stop you there?

You said, Mr. Potts, that the incident was serious. Can you give me an example of a business or an individual who has been taken off the Facebook platform for the type of incident or breach that happened involving Aleksandr Kogan, the sharing of information?

Mr. Neil Potts: I think that you just named one. Mr. Lucas, I don't work on those issues directly, the privacy issues. Those go through a separate team.

I do want to say that we are committed, as Mr. Chan said, to getting back to you. I've had the pleasure of giving testimony in evidence before a committee recently and—

● (1240)

Mr. Ian Lucas: I'm sorry, Mr. Potts. We want basic honesty, which is a universal value, and you have people from around the world at this table. We all understand honesty. We've got different legal systems—

Mr. Neil Potts: I fully—

Mr. Ian Lucas: —and I want straight answers. I've heard from you four times in evidence.

Mr. Neil Potts: Mr. Lucas, I fully agree with you about honesty and—

The Chair: I'm sorry Mr. Potts—

Mr. Neil Potts: —and to impugn somebody's integrity, it is a strong action.

The Chair: Mr. Potts, the priority is given to members of the committee, and Mr. Lucas has the floor.

Go ahead, Mr. Lucas.

Mr. Ian Lucas: I have not had a straight answer from your company. You've been sent here by Mr. Zuckerberg to speak on behalf of Facebook. He's had plenty of notice of these questions.

Mr. Kevin Chan: I'm sorry, sir, let me just.... If I understand correctly, your question was: Are there other apps that have been banned from the platform for inappropriate use or abuse of the platform? The answer is yes.

Mr. Ian Lucas: For transferring data....

The Chair: We're at time, so I have to move on to the next questioner, who is Mr. Lawless from Ireland.

Mr. James Lawless (Member, Joint Committee on Communications, Climate Action and Environment, Houses of the Oireachtas): Mr. Chair, thanks for including us here today. I'm glad to be here.

We've had engagement, obviously, at our Irish committee with the companies and we met Mr. Zuckerberg in Dublin recently.

I have to say that I welcome the engagement of the representatives from the tech companies that are here, but I do find extraordinary some of the statements that have been made, such as the statement made by Mr. Potts a few minutes ago that he wasn't familiar with the parliamentary procedure, and that was maybe to explain some gap in the evidence.

I also find it extraordinary that some of the witnesses are unfamiliar with previous hearings and previous discourse on these matters in all of our parliaments. I would have thought that was a basic prerequisite before you entered the room, if you were qualified to do the job. I caveat my questions with that. It is disappointing. I want to put that on record.

Moving on to the specifics, we've heard a lot of words, some positive words, some words that are quite encouraging if we were to believe them, both today and previously, from the executive down. However, I suppose actions speak louder than words—that's my philosophy. We heard a lot today already about the Cambridge Analytica-Kogan scandal. It's worth, again, putting on record that the Irish data protection commissioner actually identified that in 2014 and put Facebook on notice. However, I understand that it wasn't actually followed up. I think it was some two or three years, certainly, before anything was actually done. All that unfolded since could have been avoided, potentially, had that actually been taken and followed up on at the time.

I'm following that again to just, I suppose, test the mettle of actions rather than words. These first few questions are targeted to Facebook.

We heard Mr. Zuckerberg say in public, and we heard again from witnesses here today, that the GDPR is a potential gold standard, that the GDPR would be a good model data management framework and could potentially be rolled out worldwide. I think that makes a lot of sense. I agree. I was on the committee that implemented that in Irish law, and I can see the benefits.

If that is so, why is it that Facebook repatriated 1.5 billion datasets out of the Irish data servers the night before the GDPR went live? Effectively, we have a situation where a huge tranche of Facebook's data worldwide was housed within the Irish jurisdiction because that's the EU jurisdiction, and on the eve of the enactment of GDPR —when, of course, GDPR would have become applicable—1.5 billion datasets were taken out of that loop and repatriated back to the States. It doesn't seem to be a gesture of good faith.

Perhaps we'll start with that question, and then we'll move on if we have time.

Mr. Kevin Chan: Thank you very much, sir.

I very much agree with you that actions speak louder than words. I think that, to the degree that we need to demonstrate that, we will be working in the coming months and in the coming years through our actions to demonstrate that we intend to keep our service secure and the privacy of individuals safe, and that we intend to do the right thing.

In terms of what you mentioned with respect to the transfer.... Again—full declaration—I am not a lawyer, but I understand that's consistent with our terms of service.

Mr. James Lawless: It's consistent, but it's also incredibly convenient that it was on the night before the GDPR became effective.

I'll ask another question in the same vein. My understanding is that Facebook is continuing to appeal a number of decisions. The U. K. information commissioner had a negative finding against Facebook recently, which Facebook is appealing. My colleague, Hildegarde Naughton, has talked about the Irish data protection commissioner's findings.

If you're putting your hands up and saying, “We got some things wrong”, and demonstrating good faith, which I would welcome if that were the case, why are you continuing to appeal many of these decisions?

● (1245)

Mr. Kevin Chan: There are instances.... Because they are subject to court processes, there are limits to what I think we can say today. As you are probably aware, we are trying very hard to arrive at resolutions on other open matters. I think that I would urge you to observe our actions as we can make them public through these processes and make a determination at that time.

Mr. James Lawless: I just have a very quick question for Google.

I understand that Google's approach has been to not run political advertising at all, certainly in the Canadian context. We saw a similar decision in Ireland during the abortion referendum a year ago. I have concerns about that decision because I think that it allows malevolent actors to take the stage in terms of misinformation that's not targeted. I think that perhaps it's actually more bona fide to have political actors be transparent and run ads in a legitimate, verified context.

I'm just concerned about that, and I hope that's not going to be long term. Maybe that's an interim move.

Mr. Colin McKay: With the few seconds we have left, I have an observation. Both in Ireland and in Canada, we found ourselves in a position where we were seeing uncertainty in what we could guarantee to the electorate. We wanted to make sure we had a strict framework around how we were serving advertising and recognizing our responsibilities. As my colleague mentioned earlier, a goal of ours moving forward is that we have the tools in place so that, whether it's a question of ambiguity or malevolent actors, there is transparency for users and it's done in a clear and consistent way across all our products.

The Chair: Thank you, Mr. Lawless.

We'll go into our next round now.

Go ahead, Singapore.

Ms. Sun Xueling (Senior Parliamentary Secretary, Ministry of Home Affairs and Ministry of National Development, Parliament of Singapore): I would like to come back to the example of Sri Lanka, with Mr. Neil Potts.

Mr. Potts said earlier that he was not aware that the incendiary videos had been sent up to Facebook. I would like to highlight that in an article in The Wall Street Journal, Mr. Hilmy Ahamed, Vice-President of the Muslim Council of Sri Lanka, said that Muslim leaders had flagged Hashim's inflammatory videos to Facebook and YouTube using the services that were built into your reporting system.

Can I just confirm with Mr. Potts that if you were aware of these videos, Facebook would have removed them?

Mr. Neil Potts: Yes, ma'am. That's correct. If we are aware, we would remove the videos. With this specific case, I don't have the data in front of me to ensure we were put on notice, but if we were aware, these videos would have been removed.

Ms. Sun Xueling: Thank you.

Similarly, can I then confirm in the same spirit that if Facebook were aware of a video being falsified—and we discussed the case of Nancy Pelosi earlier—Facebook would then carry a clarification that they are aware the video is falsified?

Mr. Neil Potts: When one of our third party, fact-checking partners.... We have over 50 now who are international, global and that adhere to the Poynter principles. They would rate that as being false. We would then put up the disclaimer. We would also aggressively reduce that type of information and also signal to users who are not only engaging with it but trying to share, or have shared, that it has been rated false.

Ms. Sun Xueling: Your disclaimer would actually say that you understand that the information contained is false.

Mr. Neil Potts: It would have a link or a header to the article from one of the fact-checkers that disputes and claims it is false.

Ms. Sun Xueling: This would be circulated to all who would have seen the original video.

Mr. Neil Potts: If you are engaging with it currently, you would see it, whether at the bottom in your newsfeed or perhaps on the side if you are on desktop. If you have shared it, you would be informed that there has been an action disputing the validity of the content.

Ms. Sun Xueling: Mr. Chan, previously you had talked about Facebook putting friction into the system. Can I then confirm with you that Facebook is committed to cutting out foreign interference in political activities and elections, and that you would actively put friction into the system to ensure that such foreign interference is weeded out?

Mr. Kevin Chan: I suspect you're asking about potential legislation in Singapore. You would be well served to look at the Elections Modernization Act that Canada put in place—

Ms. Sun Xueling: My question was quite specific. I wanted you to confirm what you said earlier, that you are putting "friction" into the system. You specifically used that term.

Mr. Kevin Chan: Parliament has given us great guidance and we have decided to put friction into the system. We would recommend that the Canadian model be something that you consider as you develop legislation elsewhere.

● (1250)

Ms. Sun Xueling: Thank you.

The Chair: We've gone through just about all the delegates. We're going to go back to the U.K. for another kick. You didn't have to share your time, so we're going to give you some more time.

We're going to go to Mr. Erskine-Smith, and I think Mr. Angus has another question. Ms. Stevens...again, and then I think we've completed everybody.

As chair, I'm going to try to give everybody a five-minute turn. Once we have gone through everybody, we have David to follow the sequence. Then we'll look at second questions in second five-minute times, so if you wish to ask another question, please let the chair know, and I'll try to put them in priority.

Next up, we have Mr. Erskine-Smith.

Mr. Nathaniel Erskine-Smith: Thank you very much.

I just want to pick up where I left off with Google. Would you support a competition framework that includes privacy in the competition commissioner's purview?

Mr. Colin McKay: We have two regulatory mechanisms in Canada, one for competition and one for data protection. This was highlighted in the government's recent digital charter. They've both been identified for review over the next year and that's a process where I think we can discuss that balance.

Mr. Nathaniel Erskine-Smith: So Google doesn't have a view right now. Okay.

To Twitter...and I ask this partly because our competition commissioner, unbeknownst to Facebook in particular, on Thursday is engaged in this very conversation. It's not just the German regulator. They're holding a data forum at the National Arts Centre.

Does Twitter have a view of competition policy and privacy?

Mr. Carlos Monje: Thank you for the question, and thank you also for distinguishing the platforms that are on here. Twitter has a single-digit share of the advertising market. We have 130-odd million daily users. We treasure them all. We work to keep their trust and to keep them engaged, and are closely watching these antitrust and competition—

Mr. Nathaniel Erskine-Smith: Do you agree that privacy should play a central role in competition law?

Mr. Carlos Monje: I'd have to examine that a little bit more closely.

Ms. Michele Austin (Head, Government and Public Policy, Twitter Canada, Twitter Inc.): We would echo the same comments said by Google. We would look forward—

Mr. Nathaniel Erskine-Smith: So you have no view right now.

Ms. Michele Austin: —to working on the marketplace framework, which is the basis of competition law.

Mr. Nathaniel Erskine-Smith: Right. Okay, so none of you have a view on a really important issue of our day.

In terms of algorithmic accountability, the Government of Canada now has algorithmic impact assessments. Have any of your companies conducted algorithmic impact assessments? Facebook for News Feed, Google for the recommendation function on YouTube, and Twitter, have you conducted internal algorithmic impact assessments, yes or no?

Mr. Kevin Chan: I think broadly, yes. I don't know exactly what you mean, but if you're asking if we have a work stream to understand the implications of algorithms—

Mr. Nathaniel Erskine-Smith: To understand a risk assessment of positive and negative outcomes of the algorithms that you're currently employing on millions of people....

Mr. Kevin Chan: Sir, not only do we have a team on it internally. We also have an international working group of experts on algorithmic bias that we convene on a regular basis to discuss these matters.

Mr. Nathaniel Erskine-Smith: Your company has never had analysts look at the News Feed, and the algorithms that are employed on that News Feed, and said here are the positive and negative outcomes that we should be considering.

Mr. Kevin Chan: I thought I just answered in the positive.

Mr. Nathaniel Erskine-Smith: So you have. Okay.

Google, with respect to the YouTube recommendation function...?

Mr. Derek Slater: Similarly, we're constantly assessing and looking to improve.

Mr. Nathaniel Erskine-Smith: You have internal documentation that says these are the positive outcomes, these are the negative outcomes, and this is the risk assessment with respect to the algorithms we employ. Is it fair to say you have that?

Mr. Derek Slater: We constantly do that sort of assessment, yes.

Mr. Nathaniel Erskine-Smith: Great.

And Twitter, is it the same?

Mr. Carlos Monje: We are assessing it. I'd also note that Twitter's use of algorithms is substantially different. People can turn it off at any point.

Mr. Nathaniel Erskine-Smith: Would you provide the internal risk assessments to this committee?

Mr. Derek Slater: Speaking for ourselves and the YouTube recommendation algorithm, we continue to try to improve the transparency that we have.

Mr. Nathaniel Erskine-Smith: Would you provide those internal risk assessments? They ought to be public, frankly, as far as I'm concerned, in the same way the Government of Canada has an algorithmic impact assessment and any departmental agency that wants to employ an algorithm has to be transparent about it. None of you billion-dollar companies have to be, and I think you should be.

Would you provide to this committee the algorithmic impact assessments, which you've said you have done, and engage in some transparency?

Mr. Kevin Chan: I thank you for that. I think we're going to go further than that. We are in the process, as I've mentioned, of providing more transparency on a number of things that you will see on the platform. We have actually introduced in some markets already, as a test, something called WAIST, which is "Why Am I Seeing This?" That gives you a very good sense of how things are being ranked and sorted by News Feed.

Mr. Nathaniel Erskine-Smith: Because you're going to go further, I assume that it's, yes, you will provide that internal documentation to this committee.

Mr. Kevin Chan: I think we're going to do better. We're going to speak by our actions, as we talked about earlier, sir.

Mr. Nathaniel Erskine-Smith: I can't tell if it's a yes or a no.

Google...?

Mr. Derek Slater: We will continue to communicate on how we're doing.

Mr. Nathaniel Erskine-Smith: I take that as a no.

Twitter...?

Mr. Carlos Monje: We believe transparency is key. I think there are a couple of points to consider. One is that each of these algorithms is proprietary. It's important to think about those things.

Mr. Nathaniel Erskine-Smith: I understand, yes.

Mr. Carlos Monje: The other is understandable. We often talk very different languages. Bad actors, and their understanding of how we do our things...and also to judge us on the outcomes and not necessarily the inputs.

● (1255)

Mr. Nathaniel Erskine-Smith: Okay.

I'm running out of time, so I want to talk about liability and the responsibility for content on your platforms. I understand that for very harmful content...and we can talk about the nature of the content itself. If it's very harmful, if it's child porn or terrorism, you will take it down. If it's clearly criminal hate speech, you take it down, because these are harmful just by the nature of the content. There would be liability in Germany, certainly, and we've recommended at this committee that there be liability. If it's obviously hateful content, if it's obviously illegal content, there should be liability on social media platforms if they don't take it down in a timely way. That makes sense to me.

The second question, though, is not about the nature of the content. It's about your active participation in increasing the audience for that content. Where an algorithm is employed by your companies and used to increase views or impressions of that content, do you acknowledge responsibility for the content? I'm looking for a simple yes or no.

Let's go around, starting with Google.

Mr. Derek Slater: We have a responsibility for what we recommend, yes.

A voice: For sure.

A voice: Yes.

Mr. Carlos Monje: Yes, we take that responsibility extremely seriously.

Mr. Nathaniel Erskine-Smith: Thanks very much.

The Chair: We'll go back to the U.K. delegation for another five-minute slot.

Just so it's clear, Estonia has asked for a second question. Germany, Mexico and members of our committee have as well. There's Singapore, whose hand I've seen just now, Charlie Angus, Damian Collins and then I'll finish.

Mr. Lucas or Ms. Stevens, go ahead.

Mr. Ian Lucas: To all the platforms, do you have a satisfactory age verification process in place for your platform?

Mr. Monje.

Mr. Carlos Monje: We do. We implement the GDPR age gating procedures and are trying to figure out ways to do that in a way that protects the privacy of our users. Often you have to collect more information from minors in order to verify they are who they say they are.

Mr. Ian Lucas: Facebook, do you have a satisfactory age verification process in place?

Mr. Kevin Chan: I thought Carlos's answer was quite good. That's exactly the tension we're looking at.

Having said that, I understand the spirit of your question. We can always get better. I have to tell you—and I think you've heard it from colleagues of mine who recently appeared in the U.K.—

Mr. Ian Lucas: You do read transcripts of evidence, then.

Mr. Kevin Chan: Actually, I didn't. I spent time with a colleague, Karina Newton, whom members may know. She's a lovely lady and she spent some of her time briefing me on how she thought it went. She thought it went really well. There were really deep and piercing questions, sir, with respect to age verification.

Unfortunately, though, the technology is not quite there yet.

Mr. Ian Lucas: Google...?

Mr. Derek Slater: Yes, we have requirements in place and broadly agree with what was said.

Mr. Ian Lucas: You may have requirements in place, but I've actually been able to join Instagram as a 10-year-old, I think, during the course of a committee meeting. It seems to me, from the evidence I've heard and from what I hear from my constituents in the U.K., people are extremely concerned and don't believe there are satisfactory age verification processes in place. Indeed, the evidence I received was that the platforms themselves in the U.K. seemed to be suggesting there weren't satisfactory age verification procedures in place.

Do you disagree with that? Do you think the position is okay? That is basically what most of us have been asking.

Mr. Kevin Chan: Sir, what I said earlier was that we can always do better. The technology is not where we'd like it to be.

Mr. Ian Lucas: Okay.

For Facebook, I'm a little confused about the relationship you have with WhatsApp and Instagram, and the transfer of data. If I give information to Facebook, is it freely transferable to Instagram and to WhatsApp?

Mr. Kevin Chan: As you know—I believe, because Karina mentioned that you had an exchange on this in the U.K.—Facebook and Instagram are governed by one set of terms of service, and WhatsApp is governed by another.

● (1300)

Mr. Ian Lucas: That means information is shared between Instagram and Facebook.

Mr. Kevin Chan: Correct. As we discussed earlier, it is important for us to be able to leverage infrastructure in order to do a lot of the things we do to try to keep people safe. Karina kind of mentioned this, although she said she didn't know if it was completely clear. Having real world identities on Facebook actually allows us to do some of the things we wouldn't be able to do with Instagram on its own to ensure we're able to get greater certainty on these questions of age, real world identity and so on. Facebook enables us to leverage some of the security systems and apply them to Instagram, because Instagram, as you obviously know, functions quite differently and has a very different set of practices in terms of how people use the service.

Mr. Ian Lucas: Finally, to all the platforms, if you were legally responsible for the content of your platforms, would you be able to function as businesses?

Mr. Derek Slater: There are existing legal frameworks with respect to our responsibility for illegal content, which we abide by.

Mr. Ian Lucas: If it were possible to conduct legal actions against the separate platforms because of information that you circulated, which we knew could cause harm in the future, do you think you would be able to continue to trade or do you think that would put you out of business?

Mr. Carlos Monje: I'm most familiar with the American context where we do have a degree of immunity. It was under the Communications Decency Act, and it was designed to give us the flexibility to implement our terms of service so that we wouldn't get sued. America is a very litigious society, as you know, and that protection has enabled us to create and maintain a much safer platform than it otherwise would be.

What you've seen across this table and across the world are many different regimes trying different mechanisms to do that. There has been independent research about the implications of that, including places where accusations were that the platforms overcorrect and squelch good speech. In the U.S. we don't often get criticisms from government to take things down because it is a violation of our hate speech or hateful conduct policy, but rather because it is a violation of copyright law, because the copyright rules in the United States are very strict, and we have to take it down within a certain period of time.

Rather than taking somebody who is critical of the government and asking them to take it down because of other terms of service, they go to the strictest regime, and that has a very negative impact on free expression.

The Chair: Thank you.

We have to move on. I want to highlight what's going to happen in the next 30 minutes. We have two members of the Canadian committee who haven't spoken yet. We're going to give them five minutes each. That gives us, with the people who have asked for second questions, about 20 minutes, approximately three minutes per individual.

Again, we'll go to Mr. Graham first and Mr. Saini, and then we'll go by country.

Go ahead, Mr. Graham.

Mr. David de Burgh Graham (Laurentides—Labelle, Lib.): Thank you very much.

I want to get straight into this. I'm going to focus on Google and Facebook for a minute.

Do you accept the term “surveillance capitalism”, Google?

Mr. Colin McKay: I think it's an exaggeration of the situation, but it reflects social pressures and a recognition that there is an increasing worry about the data that's collected about individuals.

Mr. David de Burgh Graham: Facebook...?

Mr. Kevin Chan: I cringed, I think, when I read it the first time.

Mr. David de Burgh Graham: You track individuals on the Internet in any way, shape or form without their knowledge or explicit consent at any time for any reason, and you do so for profit.

Mr. Colin McKay: We have a pretty clear relationship with our users about what information we collect and what we use it for. We secure consent for the information that we use.

Mr. David de Burgh Graham: But you don't only track information on users. You track information on anybody on the Internet. If you look at Google Analytics and any of these other services that track anybody passing through another website that has nothing to do with Google, you're collecting vastly more data than what is provided voluntarily by users. My question is, again, are you collecting data on people for profit and, if so, is that not surveillance capitalism?

Mr. Colin McKay: I think in the broad circumstance you just described around people using the Internet, we're not collecting information about people. We're measuring behaviour and we're measuring.... Sorry, that's the wrong term. I can hear the chuckle.

We're measuring how people act on the Internet and providing data around that, but it's not around an individual. It's around an actor.

● (1305)

Mr. David de Burgh Graham: Or it's around a type of individual, an IP address or this type of information. You are collecting data that can be annexed to people. My point, and I want to take it further than that, is that governments have a tremendous surveillance capacity, as we all know. At least in this country and a lot of other countries around this table, we now have a committee of parliamentarians to oversee our security apparatus, and they go in a classified setting. They dive deeply into the intelligence agencies, what they do, how they do it and why, and they report it back.

If these committees were either created to just focus on social media companies or this committee was applied to it, what surprises would they find?

Mr. Kevin Chan: Sir, as I've indicated, we want to do more than that by our actions. We're going to make all of that available and then people can...including things that are off platform. If there's a site that uses, let's say, a plug-in or something like that from Facebook, you have available all that information and you can do whatever it is you want with it. You can remove things. You can delete things. You can transfer it. You can download it. That is our commitment and we will be moving fast to get it done.

Mr. David de Burgh Graham: I appreciate that, but if you go into Facebook and ask it to download your data, the data that it gives you is not a comprehensive collection of what Facebook has on you as a user.

Mr. Kevin Chan: Right. I think you're referring to when you download your information you get things like the photos and the videos.

Mr. David de Burgh Graham: You get a handful of your pictures, a handful of your updates and have a nice day.

Mr. Kevin Chan: That's right. What we want to do is build...and it takes a bit of time. If you can bear with me, it takes a little bit more time to build something that's much more ambitious, which is to then give you actual control over not just the things that you put on Facebook but all the activity that you may have done with social plugs-ins elsewhere, where we can give you the ability to control and remove stuff if you so choose.

Mr. David de Burgh Graham: If Mark Zuckerberg were to run for president of the United States, for example, what limits his ability to use Facebook's data, machines, algorithms and collection to feed his campaign?

Mr. Kevin Chan: Sir, if I may, that is a very good question, and that's precisely why we have the policies that we have in place and why we hold so steadfastly to them. It's not...and I think the question kind of came about in a different way. It was, “What if there was a photo of Mark Zuckerberg or a video of Mark Zuckerberg?” The treatment would be the same. That's because these policies have to hold regardless of the direction the wind blows.

As I said before, we understand that people may not be comfortable with the degree of transparency and the degree to which Facebook is able to make these decisions about what happens on our service, which is why we're building this external oversight board, so that these decisions, so that many of these hard precedential decisions, will not be made by Facebook alone. There will be an ability to appeal to an independent body that can make these decisions that would govern the speech on a platform.

Mr. David de Burgh Graham: I only have seconds, and I want to come back to the independent body in a second.

My point is, if Neil Potts runs for president of the United States and Mark Zuckerberg runs for president of the United States, I suspect that the support from Facebook and the data usage from Facebook would not be the same. On that basis, it would be very hard to say that having Mark Zuckerberg and Neil Potts here is equivalent.

Mr. Kevin Chan: Again, our policies are for everyone. We would not make any exceptions for anybody, which is in fact why we have these kinds of robust conversations.

Mr. David de Burgh Graham: Does Mr. Zuckerberg have a—

The Chair: We're actually out of time. Sorry, Mr. Graham.

We'll go to Mr. Saini for five minutes.

Mr. Raj Saini (Kitchener Centre, Lib.): Good afternoon.

One of the things we've heard from many experts is that a lot of the issues that have happened with data were when the machine learning really came into force. There was an inflection point. Many experts agree that self-regulation is not viable anymore. Rules have to be in place. The business model just can't regulate itself, and it doesn't align with the public interest.

I have two points. My concern is that right now, we're a mature democracy. A lot of the countries represented around this table are mature democracies. My worry is for nascent democracies that are trying to elevate themselves but don't have the proper structure, regulation, education and efficiency in place, or a free or advanced press. There has been some suggestion that maybe this self-regulation should be internationalized, as with other products. Even though some countries may not have the ability to effectively regulate certain industries, the mature democracies could set a standard worldwide.

Would that be something that would be accepted, either through a WTO mechanism or some other international institution that's maybe set apart? Part of the conversation has been around the GDPR, but the GDPR is only for Europe. There are the American rules, the Canadian rules, the South Asian rules.... If there were one institution that governed everybody, there would be no confusion, wherever the platforms were doing business, because they would accede to one standard worldwide.

● (1310)

Mr. Kevin Chan: You are correct. Where we can have harmonization of standards across the world, that's helpful. We've called for that in multiple realms, including in the privacy realm.

I would say that's actually one of the key challenges. It's a vigorous debate that we have when we talk about the oversight board. In the consultations we've had around the world, including in Canada, the big question that's come up is, “How can you have a global board make decisions that have local impact?” It's come up, and I can say we've had some interesting conversations with the Assembly of First Nations. Obviously they have some unique questions about what the right governing framework is for content online and how we marry the international with the local.

I absolutely agree with you, sir. That's a very good and astute question, and one that we wrestle with.

Mr. Raj Saini: Google...?

Mr. Colin McKay: This is a challenge we've recognized since the early days of implementing machine learning in our products, and it's one of the reasons we came out over a year ago with a very clear set of principles around how we will use artificial intelligence in our products.

We certainly underline that there needs to be an active conversation between industry and governments around the world. In the past, this sort of principles-based development of regulation that was led by the OECD around data protection has served us well for developments according to region and in levels of sophistication.

I agree with you that this sort of principles-based global collaboration, especially in concert with the companies that will have to execute on it, will result in a fairer regulatory system that's as broadly applicable as possible, whether in this room or globally.

Mr. Raj Saini: Thank you for that. Obviously you're going to take in the local effect of any country you work in, but there are some basic principles that I think can be agreed upon worldwide.

My final question is a bit philosophical but also a bit practical. In certain countries in which you operate, you know there are no standards and no regulation. The rule of law is lacking, a free press is lacking and the government structure is not that advanced. The content could be exploited in a much more heinous or worse way in those countries than in other parts of the world.

Is there no moral incumbency on the platforms to make sure that when they go into those jurisdictions they are helping to elevate the governance structure, so that when they're doing business in those countries, it's done in a more equitable manner?

Mr. Colin McKay: I have a twofold response to that.

First, as my colleague, Mr. Slater, mentioned, we work very hard to make sure the policies and guidelines around all of our products apply to circumstances in those countries as well as what we might describe as more developed or more stable countries.

However, that's also why people like me work at the company. We work on teams that focus on AI and on privacy and data protection. We have those engagements, whether in the country itself or at international organization meetings, so that we can have an ongoing conversation and share information about how we're seeing these policies and technologies develop internationally. We can provide a comparison with how they're seeing that develop within their own jurisdiction.

It's an honest and forthright exchange, recognizing that we're on the forefront of a technology that is having a significant impact on our products and a significant benefit for our users.

Mr. Raj Saini: Thank you very much.

The Chair: Thank you, Mr. Saini.

Now, we'll go into the countries again. We're at about two minutes each. If it can be quick that would be great. We have Estonia, Germany, Mexico, Singapore, Ireland and then we have some closing statements from us.

Go ahead, Estonia.

Ms. Keit Pentus-Rosimannus: Thank you.

It has been pointed out that the disinformation phenomenon is becoming more complex and cross-channel or cross-platforms, meaning that the different phases or different stages of the disinformation campaigns happen often on different channels.

How do you co-operate? How do you see what could be the model for co-operation between the different platforms in order to fight the disinformation problem?

Mr. Derek Slater: We do our own threat assessments to prevent and anticipate new trends, and then we work collaboratively among the industry, and where appropriate with law enforcement and others, to make sure information and indicators are shared. We actively want to be a participant in that sort of process.

Mr. Carlos Monje: I'll just say that the companies do work together on these issues and work closely with governments. In Mr. Saini's comments, I was thinking about the role of government and how forward-leaning Estonia has been, under the thumb of Russian disinformation for a long time, in working to improve media literacy and working with the platforms in a way that it makes our jobs easier.

Everyone has a role and the companies do work together to try to address common threats.

● (1315)

Mr. Neil Potts: A good place to perhaps look is the work that we do as the Global Internet Forum to Counter Terrorism. All of our companies are members of that forum, where we have shared responsibilities of information sharing, technological co-operation and then support for research.

The Chair: Next up is Germany.

Go ahead.

Mr. Jens Zimmermann: Thank you, Mr. Chairman.

I would like to ask a few questions of Twitter.

During the recent European elections you introduced several measures, especially concerning fake news about the electoral process as such. That sounded like a good idea in the first place, but we ended up having elected officials in Germany being blocked for tweets that obviously didn't have any failed information in them.

Obviously, the complaint mechanism from Twitter was used by right-wing activists to flag completely legal posts by members of Parliament, for example. It was really the problem that you did it that way, and it took quite some time until everything was solved.

Have you monitored these developments? What are your lessons learned, and how will that evolve during upcoming elections?

Mr. Carlos Monje: Thank you for that question.

I followed that as well from the U.S., the disinformation reporting flow that we launched in the EU and in India. I think this is one of the challenges and blessings of being a global platform—every time you turn around there's another election. We have Argentina coming up. We have the U.S. 2020 elections to follow, and Canada, of course, in October.

What we learned is that, as always, when you create a rule and create a system to implement that rule, people try to game the system. What we saw in Germany was a question of how and whether you sign a ballot. That was one of the issues that arose. We are going to learn from that and try to get better at it.

What we found—and Neil mentioned the GIFCT—was that our contribution to the effort, or what Twitter does, is to look at behavioural items first, which is not looking at the content but how are different accounts reacting to one another. That way we don't have to read the variety of contexts that make those decisions more complicated.

The Chair: Thank you.

We'll go to Singapore for two minutes.

Mr. Edwin Tong: Mr. Potts, earlier you had said in answer to my colleague's question that you were not aware of being told prior to or after the bombings in Sri Lanka that it, in fact, had been flagged to Facebook prior to that. Do you recall that?

Mr. Neil Potts: Yes, sir.

Mr. Edwin Tong: This was a serious and horrific massacre where videos were carried on Facebook for some time and, as you said, it's hate speech in clear breach of your policies. The alleged bomber himself, in fact, had a Facebook account, which I'm sure you know. I'm surprised that you didn't check, because that's something that I would have thought Facebook would want to know.

They would have wanted to know how it is that, with videos having been spread on Facebook, this was something that Facebook had missed, if at all you had missed it. I'm surprised you are not aware today as to whether or not this was something flagged to Facebook. Can you confirm that?

Mr. Neil Potts: For the specific video, sir, I'm happy to follow up after this hearing, and to come back to show you exactly that timeline. When we were made aware of the attack of the individual, we quickly removed—

Mr. Edwin Tong: I know. That's not my focus. Why it is that today, about two months after the event, you still don't know if, prior to the attack, Facebook had been made aware of the existence of the videos? I would have thought that, if you were to have us believe that the policies you now have in place—AIs and other mechanisms for the future.... If I were Facebook, I would have wanted to know how this was missed. I'm surprised that you don't know, even today.

Mr. Neil Potts: That is correct. We do a formal after-action process where we review these incidents to make sure that our policies—

● (1320)

Mr. Edwin Tong: It didn't come up.

Mr. Neil Potts: I would just have to get the information back for you. I don't want to speak out of turn.

Mr. Edwin Tong: You, yourself, Mr. Potts, just last month, gave evidence to the U.K. Parliament, where this issue came up in that session. Was that not correct?

Mr. Neil Potts: I believe the attack happened on Easter Sunday. We gave evidence, I believe, on that Tuesday. It was very much in the nascent stages when we gave evidence.

Mr. Edwin Tong: Fair enough, but I would like to say that I'm surprised Facebook didn't see fit to check whether something had been missed.

Mr. Kevin Chan: If I may say, sir, there is one thing I want to assure—

Mr. Edwin Tong: If it's an answer to my question, then, yes, please explain, but otherwise—

Mr. Kevin Chan: It's about our security posture, sir.

The Chair: I'm sorry. If it's not an answer directly to Mr. Tong, we don't have the time.

I'm sorry, Mr. Tong. We're out of time.

We have to move on to Ireland for two minutes, and then we will make some closing remarks.

I apologize. I wish we had more time. We just don't.

Go ahead.

Ms. Hildegarde Naughton: Thank you, Mr. Chair.

I didn't have a chance to get the answer to my first question in relation to Google's viewpoint on the GDPR. Many of the social media companies are based in Ireland. Effectively, our data protection commissioner is regulating for Europe, and Facebook's Mark Zuckerberg has called on a GDPR-type approach to be rolled out globally.

What is your view on that? Will it work?

Mr. Colin McKay: We think the GDPR provides a strong framework for a conversation around the world on what extended privacy protections would look like. The question is how it adapts to local jurisdictions, and also reflects the political and social background of each of those jurisdictions.

Ms. Hildegarde Naughton: You can't be definitive about whether it would work.

Are you in agreement with Mr. Zuckerberg in relation to the rollout of GDPR globally?

Mr. Colin McKay: We've already made a broad and detailed statement about the need for increased work on privacy regulation. It was last fall. It builds on a lot of the work around the development of GDPR.

I'm just being careful, because I recognize that, around the table, there are many different types of data protection regulations in place right now.

Ms. Hildegarde Naughton: In different countries....

In relation to Ireland yet again, because it's the base of a lot of the social media companies.... You're all based, your European international headquarters are based in Ireland. We're working on digital safety commissioner legislation, which will effectively mean that Ireland will be legislating in relation to takedown online content moderation for Europe, and potentially beyond that.

Is that how you would see it? What is your viewpoint on that, very briefly?

Mr. Derek Slater: Consistent with what we said at the outset, clear definitions by government of what's illegal, combined with clear notices, are critical to platforms acting expeditiously. We welcome that sort of collaboration in the context of illegal content.

Ms. Hildegarde Naughton: Can you see that being rolled out, maybe beyond Europe, because of the legislation in Ireland.

Mr. Derek Slater: Whether or not it's that specific law, I think the basics of notice and take down of illegal content, speaking broadly, is something there is increasing consensus around.

Ms. Hildegarde Naughton: Facebook, do you want to come in on this?

Mr. Kevin Chan: I think what Mr. Slater said is absolutely right. We do want to work with you. I understand our team is, in fact, working with the Irish public authorities on this.

We are also working with President Macron and the Government of France on what he's calling smart regulation. We would welcome, I think, the opportunity to discuss with you and others in Ireland how that is evolving. I think it's worth having additional conversations on it.

Mr. Carlos Monje: In addition to the importance of having precise terminology, I think accountability is important, beyond the regulatory agency to the Parliament and the people who can be held accountable by their constituents.

I would also note that it's important, especially on these issues of content moderation, which we take extremely seriously, to recognize how those tools can be used in the hands of autocratic regimes. I was listening to the testimony yesterday about pre-Nazi Germany. The tools used there to protect democracy in one case were then used to squelch it on the back end. I think they are difficult questions and I'm glad that this committee is taking it so seriously.

The Chair: Thank you, Ms. Naughton.

We appreciate all the testimony today.

We have some closing statements, starting with Mr. Angus....

My apologies to Mexico, you did put up your hand, so we'll give you a quick two minutes. Go ahead.

Hon. Antares Guadalupe Vázquez Alatorre: [*Delegate spoke in Spanish, interpreted as follows:*]

I just briefly would like to ask you, what is the path that a victim must follow when the controls fail that are going against [*Technical difficulty—Editor*] and Google in particular.

Mr. Derek Slater: If I understand correctly, before you were asking about content that violates our community guidelines on YouTube. We have flagging systems where a user can click and say, "This violates your guidelines in this particular way." That notice is then sent and put into a queue for review. They can do that right under the video there.

● (1325)

Hon. Antares Guadalupe Vázquez Alatorre: [*Delegate spoke in Spanish, interpreted as follows:*]

What happens when they are told that there is no breach in the policies, and there is a video with a person who is naked and everybody can see that?

Mr. Derek Slater: From the context, if it violates our guidelines, we would remove it. If we don't, there are appeal mechanisms, and so on and so forth.

Hon. Antares Guadalupe Vázquez Alatorre: [*Delegate spoke in Spanish, interpreted as follows:*]

I know of cases, many cases, that have followed all the routes online and always the answer has been, "This is not against our policies," on the three platforms. What does the victim do? How do they appeal to anybody?

As I told you, in a particular case, when they went to the Google office in Mexico, they were told to go to Google in the United States. Therefore, what does a victim do when the images against that person still appear? They are up there.

Mr. Derek Slater: I'm not familiar with the particular cases you're talking about, but we'd be happy to follow up.

Hon. Antares Guadalupe Vázquez Alatorre: [*Delegate spoke in Spanish, interpreted as follows:*]

In any case, what's next?

Mr. Derek Slater: In general, if something were to violate someone's privacy or be defamatory or incite violence, and so on and so forth, against our guidelines, we would take it down. The case you're describing is something I'm not familiar with, but we'd be happy to receive more information and take it back to our teams.

The Chair: We'd better move on.

We'll go to Mr. Angus for just a couple of minutes, and then Mr. Collins and me.

Go ahead, Mr. Angus.

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

I want to make a confession. I'm a recovering digital utopian. I came here as a young democratic socialist and I fought hard against regulation. Imagine that, because we saw all the start-ups and we saw a great digital future. That was 2006. Now in 2019, I have conservative chairs here who are pushing for government regulation. That's the world we're in with you folks.

It's because we're talking about democratic rights of citizens, re-establishing the rights of citizens within the realm that you control. We're talking about the power of these platforms to up-end our democratic systems around the world, which is unprecedented. We're talking about the power of these platforms to self-radicalize people in every one of our constituencies, which has led to mass murder around the world. These are serious issues. We are just beginning to confront the issues of AI and facial recognition technologies and what that will mean for our citizens.

It's what our Privacy Commissioner has called the right of citizens to live free of surveillance, which goes to the heart of the business model, particularly of Facebook and Google, and it came up yesterday and today from some of the best experts in the world that the front line of this fight over the public spaces and the private lives of citizens will be fought in the city of Toronto with the Google project.

Mr. McKay, we asked you questions on Sidewalk Labs before, but you said you didn't speak for Sidewalk Labs, that it was somehow a different company.

Mr. Slater, we had experts say this is a threat to the rights of our citizens. Mr. McNamee said he wouldn't let Google within 100 miles of Toronto.

How is it that the citizens of our country should trust this business model to decide the development of some of the best urban lands in our biggest city?

Mr. Derek Slater: I, too, do not work for Sidewalk Labs. You're right. We want your trust, but we have to earn your trust, through transparency, through development of best practices with you and accountability. I think then different sites will make different choices. That is in general the case, but I can't speak to that specific company because I'm not a part of it.

The Chair: Thank you, Mr. Angus.

Mr. Collins.

Mr. Damian Collins: Thank you.

I would just like to pick up on a couple of things that were touched on in this session.

Mr. Potts, you mentioned briefly the changes to the Facebook Live policy as a result of the Christchurch attack. I understand that as a restriction on people who have broadcast the most serious footage through Facebook Live, and who would then have their accounts automatically suspended. Is that correct?

Mr. Neil Potts: That part is correct, but also, I think, more broadly, if you have a community standards violation for specific types of actions, you would lose your access for a period of time—30 days, 60 days, 90 days—to enable yourself to go on the live product.

● (1330)

Mr. Damian Collins: You wouldn't be able to use the live product.

Mr. Neil Potts: Correct.

Mr. Damian Collins: Would that be at a maximum of 90 days suspension?

Mr. Neil Potts: I think for egregious violations of our community standards, we also reserve the right to disable your account.

Mr. Damian Collins: Okay.

What about people who have shared serious content that has been broadcast through Facebook Live? They're not the broadcaster themselves, but they've shared that footage with others on the platform. Is there any action taken against them?

Mr. Neil Potts: We try to look at the intent of the sharer. I think that in the Christchurch example, we had many people just sharing for awareness purposes. We had some, definitely, who were sharing for malicious purposes, to subvert our policies, to subvert our AI. Those would be actioned against. If we knew that you were sharing—even media companies shared the video—we would try to read in some context and try to understand the intent of why you were sharing.

Mr. Damian Collins: Did people who you believe maliciously shared the footage have their accounts cancelled?

Mr. Neil Potts: In some cases there have been individuals who had their accounts disabled. In other cases they received penalties.

Mr. Damian Collins: Would you be able to write to us to tell us how many accounts have been disabled as a consequence of this?

Mr. Neil Potts: I'd be happy to follow up after the hearing.

Mr. Damian Collins: These changes obviously take retrospective action against people who have done it. Is there anything Facebook has done to stop something like Christchurch from happening again, in terms of the way it is broadcast and shared through your systems?

Mr. Neil Potts: We are continuing to invest in the AI.

In the Christchurch case, the use of the first-person video from the GoPro is very difficult for AI to recognize. We're continuing to invest to try to get better, to try to give training data to the machine learning so that we can identify and prevent. We have introduced new protocols for routing those types of videos to human reviewers in the moment, but it's important to note that the actual video was never reported while it was live.

Mr. Damian Collins: Okay. I'm not sure I'm clear on that, but there are a couple of more things.

You've said quite a lot about the deletion of inauthentic accounts. Facebook, I believe, said that there were 3.3 billion inauthentic accounts deleted over the previous six months. That is considerably greater than the active user base of the company. Based on that, how confident can you be that there are only about 5% of accounts at any one time that are inauthentic?

Mr. Neil Potts: We have data science teams that study this closely, so I defer to their expertise and analysis on that.

Mr. Damian Collins: Monika Bickert said that the inauthentic accounts are far more likely to be sharing disinformation, so of those 3.3 billion accounts, how many of those were actively sharing disinformation?

Mr. Neil Potts: I do not have that figure. I believe she said that they are more likely to...a combination of abusive behaviour, so not only disinformation but hate speech. Your point is taken and I can follow up.

Mr. Damian Collins: Would Facebook be able to write to the committee with the answer to that question?

Mr. Kevin Chan: Well, sir, I should clarify. I think it is the case, if you look at the transparency report—

Mr. Damian Collins: So sorry, sir, we're running out of time.

I just want to say, if you don't have the answer to that question now—

Mr. Kevin Chan: We do have the answer, sir.

Mr. Damian Collins: —the company can write to us with it.

Mr. Kevin Chan: The vast majority of accounts are actually disabled before a human can even interact with them.

Mr. Damian Collins: Okay.

Could Facebook commit to the write to the committee to say—

Mr. Neil Potts: We will write.

Mr. Damian Collins: —how many of those accounts that were deleted, those 3.3 billion, were sharing disinformation? The company is saying that they're more likely to be sharing disinformation than other sorts of accounts.

Mr. Neil Potts: If we have [*Inaudible—Editor*].

Mr. Damian Collins: Finally, in the wake of the Cambridge Analytica scandal last year, Facebook announced that there would be a new feature for users to be able to clear their browser history. I understand that Facebook announced that this will launch later this year. This does seem to be a long period of time. If this were a product launch that Facebook would be making money out of, one sort of feels it would have come on quicker. This doesn't seem to be a case of moving fast and breaking things, but of moving slowly.

Is Facebook able to commit to a date when the "clear browser history" function will be live?

Mr. Kevin Chan: Sir, I think I've mentioned it a few times, including, I think, with various members about this new feature. It would probably be inadvisable for me to commit to a date, obviously, at this time. I don't want to get out ahead of my skis, but I could just say that even with the transparency measures we're putting in place in Canada, we are working down to the wire to get this right. We're going to try to roll this other product out globally. That will take—

Mr. Damian Collins: I would just say, these sorts of functions are pretty widespread across the web. I think the fact that it's now been over a year since this was announced and that you can't even give a date this year when it will come into force is really poor.

Mr. Kevin Chan: I appreciate that.

The Chair: I want to thank everybody for your testimony today.

I applaud Mr. Chan on some of the changes that you say are coming. We've heard this story many times, so I guess we will wait to see what we get at the end of the day.

It goes to what we were asking for in the first place. In good faith we asked your CEO and your COO to come before us today to work together for a solution to what these problems are that a whole bunch of countries and a whole bunch of people around the globe see as common issues. To me, it's shameful that they are not here today to answer those specific questions that you could not fully answer.

That's what's troubling. We're trying to work with you, and you're saying you are trying to work with us. We just had a message today that was forwarded to me by my vice-chair. It says, "Facebook will be testifying at the International Grand Committee this morning. Neil Potts and Kevin Chan will be testifying. Neither of whom are listed in this leadership chart of the policy team's 35 most senior officials".

Then we're told you're not even in the top 100. No offence to you individuals, you're taking it for the team for Facebook, so I appreciate your appearance here today, but my last words to say before the committee is shame on Mark Zuckerberg and shame on Sheryl Sandberg for not showing up today.

That said, we have media availability immediately following this meeting to answer questions. We're going to be signing the Ottawa declaration just over here so we're going to have a member from each delegation sitting here as representatives.

After that, all the members of Parliament visiting from around the world are invited to attend our question period today. I'm going to point out my chief of staff, Cindy Bourbonnais. She will help you get the passes you need to sit in the House if you wish to come to QP today.

Thank you again for coming as witnesses. We will move right into the Ottawa declaration.

The meeting is adjourned.