HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

# Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 122 • 1st SESSION • 42nd PARLIAMENT

**EVIDENCE**

## Tuesday, October 23, 2018

---

## Chair

**Mr. Bob Zimmer**

# Standing Committee on Access to Information, Privacy and Ethics

**Tuesday, October 23, 2018**

● (1140)

[*English*]

**The Chair (Mr. Bob Zimmer (Prince George—Peace River—Northern Rockies, CPC)):** I call the meeting to order.

Welcome, everybody, to the Standing Committee on Access to Information, Privacy and Ethics, meeting 122. Pursuant to Standing Order 108(3)(h)(vii), we are studying the breach of personal information involving Cambridge Analytica and Facebook.

Today we have Mr. Colin McKay again, from Google Canada.

Please go ahead. You have 10 minutes.

**Mr. Colin McKay (Head, Public Policy and Government Relations, Google Canada):** Thank you very much, Mr. Chair and members of the committee. Thank you for the invitation to appear today to speak again about these important topics.

At Google we believe in ensuring that our users have choice, transparency and control. These values are built into every product we make. We build products for everyone and make most of them free.

Privacy is also for everyone, and should be simple to understand and control. At Google we combine cutting-edge technology with data to build products and services that improve people's lives, help grow the economy, and make the web safer. With partners, we are working to tackle big challenges and enable scientific breakthroughs.

We understand that our users trust us to share information about them so that we can build better products and serve and improve their lives, but we also know that with that comes great responsibility. That's why we do so with strong privacy and security practices.

Before I provide an update on important work that's happened on our end since I appeared before this committee in May, I want to briefly outline the four key pillars that underpin how Google thinks about protecting user data—transparency, control, data portability and security.

First, on transparency, our approach to privacy stems directly from our founding mission, which is to organize the world's information and make it universally accessible and useful. That's why we build for everyone. Providing most of our products for free is a key part of meeting that mission. Ads help us make that happen. With advertising, as with all our products, users expect us to keep their personal information confidential and under their control.

We do not sell personal information. This is really important. I want to repeat that point: We do not sell personal information. We strive to be up front about the data we collect, why we collect it, and how we use it. This starts with intuitive product design, ensuring that our privacy policy is clear and concise, and making privacy controls immediately accessible from the privacy policy. We also look for ways to add transparency into our products directly so that users can understand the privacy implications of their choices in context, from how you share documents in Google Drive to understanding why you are seeing certain ads.

Second, with regard to user control, our privacy tools are built for everyone. Different people have different ideas about privacy, so we must build with that in mind. Our “My Account” centre puts these privacy and security settings in a single place, making it easy to find and set preferences.

I want to call attention to our security checkup and privacy checkup tools that we regularly promote to users. These tools help users identify and control the apps that have access to their Google account data and guide users to review and change their security and privacy settings, such as deleting their Google activity, disabling personalized ads, or downloading a copy of their information.

Third, we believe portability is a key way to drive innovation, facilitate competition and best serve our users. That's why we've been working on it for over a decade. If a user wants to try out or even switch to another product or service, they should be able to do so as easily as possible and not be locked in to a service. In 2011 we launched Google Takeout, allowing users to download their data from Google and use it with a different service. We announced an important update to that service this year. That's the data transfer project, which we developed and are now working on with leading partners in the industry to facilitate that transfer between services.

Fourth, security considerations are paramount in all of these efforts. Securing the infrastructure that provides Google services is critical in light of the growing and sophisticated nature of many threats directed at our services and users. Google products are built at their core with strong security protections, including continuous efforts to block a range of security threats. We make technology like safe browsing available for free to other technology providers. This helps to protect Internet users on and off of Google services.

With that in mind, our privacy work is never finished. We try to learn from our mistakes and don't take our success for granted. Our goal is to be the best in class and continually raise the bar for ourselves and industry.

This committee's current inquiry stems from the breach of personal information that was associated with Cambridge Analytica, a breach that Facebook first reported earlier this year. When this news broke, Google proactively embarked on an analysis of our products and services to further improve the privacy of our products, particularly in relation to developer access to our data. This effort, “Project Strobe”, as it's known internally at Google, has so far resulted in several important insights and actions about our platforms. More will be coming. We announced some earlier this month, but in the interest of updating this committee on what's happened since we last spoke, let me offer a quick overview of actions that we've recently taken.

The first update is with regard to app permissions. We announced an update earlier this month outlining how consumers will now get more fine-grained control over what account data they choose to share with each app.

● (1145)

We launched more granular Google account permissions that will show in individual dialogue boxes when you download an app and when that app is updated.

People want fine-grained controls over the data they share with apps, so instead of seeing all requested permissions on a single screen, these apps will have to show you each requested permission, one at a time, within its own dialogue box. For example, if a developer requests access to both calendar entries and Drive documents, you will be able to choose to share one but not the other.

The second update concerns Gmail. We understand that when users grant apps access to their Gmail, they do so with certain use cases in mind. We're limiting the types of apps that can request access to Gmail to those that directly enhance email functionality, such as mail merge services or send-delay products.

Moreover, these apps will need to agree to new rules on handling Gmail data and will be subject to security assessments. People can always review and control which apps have access to their Google account data, including Gmail, within our security checkup tool.

The third update concerns restricting apps that can request call log and SMS permissions on Android devices. When users grant SMS, contacts and phone permissions to Android apps, they do so with certain use cases in mind.

We now limit apps' ability to receive call log and SMS permissions on Android devices and are no longer making contact interaction data available via the Android contacts API. Many third party apps, services and websites build on top of our various services to improve everyone's phones, working life and online experience. We strongly support this active ecosystem, but we understand that its success depends on users knowing that their data is secure and on providing clear tools and guidelines for developers.

From the unbundling of the permissions that are shown to users when they are deciding to give access to their sensitive data to limiting developer access to Gmail to requiring developers to undertake security enhancements, we continue to make the securing of data a top priority while supporting a wide range of useful apps.

When it comes to protecting their data and giving them more control over their data, Canadian consumers are counting on us and Canadian businesses are counting on us. Google's search tools help Canadians find information, answers and even jobs, and our advertising products help Canadian businesses connect with consumers and customers around the globe.

This brings me to one more update since I last appeared before this committee. In September, Deloitte released a report looking at the economic impact of Google Search and Google Ads on Canadian businesses. Deloitte estimates that our ads services supported between $10.4 billion and $18.5 billion in economic activity by those businesses and partners, which translates to the equivalent of 112,000 to 200,000 full-time jobs. The Android ecosystem in Canada helped generate $1.5 billion in revenue within Canada's app economy, supporting 69,000 jobs.

The web is at the heart of economic growth, both here in Canada and globally. That's why Google invests in building products and services that help businesses, entrepreneurs, non-profits, developers, creators and students succeed online. Hundreds of thousands of Canadians are using Google's tools to grow global audiences and enterprises, and we're proud to support Canadian businesses in making the most of the web.

We at Google remain committed to continuing to develop products and programs to bring this opportunity to everyone.

Our privacy and security work is never finished. We will continue to do this, and we stand ready to do our part and to help build a better ecosystem for Canadians and Canadian businesses.

Thank you again for the opportunity to be here today. I look forward to continuing to work with you on these important issues, and I welcome any questions you may have.

● (1150)

**The Chair:** Thank you, Mr. McKay.

We'll start off with Mr. Baylis for seven minutes.

**Mr. Frank Baylis (Pierrefonds—Dollard, Lib.):** Thank you, Mr. McKay, for being with us again. It's much appreciated.

I have a simple question. On average, how many data points do you collect per user? In terms of the average user, how many data points would Google have on that person?

**Mr. Colin McKay:** I can't give you an exact number for that. There is transparency around the data that's associated with you individually, in your “My Account”, the specific data that most Canadians are interested in—

**Mr. Frank Baylis:** Google collects data on, let's say, Frank Baylis.

**Mr. Colin McKay:** Yes.

**Mr. Frank Baylis:** You would have how many points on average, if I were the average user?

**Mr. Colin McKay:** I don't have an exact number for you.

**Mr. Frank Baylis:** Could you get us that number?

**Mr. Colin McKay:** Yes, I can get you that number.

**Mr. Frank Baylis:** Essentially, perhaps you could tell me how many users there are and how many data points and you can just divide it out. It's a very simple number.

**Mr. Colin McKay:** Yes.

**Mr. Frank Baylis:** I'd also like to know, since Google Home has come in, how many more data points per user there are through Google Home. Perhaps you could also provide that.

**Mr. Colin McKay:** Google Home is an extension of the services you already use. Many of your interactions with Google Home are similar to what you've already been doing on your desktop or laptop —

**Mr. Frank Baylis:** Do you track how the data points come in, whether through a phone, through Google Home, or through the search engine? Do you track, when you have these data points, how Google gets them?

**Mr. Colin McKay:** Not specifically.

If you do a search for music, that comes in under whether you have a Google Play subscription and—

**Mr. Frank Baylis:** No, I meant in Google's back offices where you have all this data on all of us. Do you know where those points come from, or do you just collect the data as is?

**Mr. Colin McKay:** I'm afraid I don't have the answer for you.

I know there's a specific.... If you're doing a voice search in your My Account, it will now tell you what the voice search was and give you a recording of it.

**Mr. Frank Baylis:** Could you let me know, then, specifically how many data points on average you have per person?

Now, you're about control and transparency. If I said I want you to give up that data, is there any way that I could ask you to not track me and to erase—I know I can erase what I see—what Google has on me? Is there any way that I have of saying "stop following me"?

**Mr. Colin McKay:** Yes. In your My Account, you can select by type of information or by service that you want that data to stop being collected and you want the record to be erased.

**Mr. Frank Baylis:** Can I ask you to delete what you've collected?

**Mr. Colin McKay:** Yes.

**Mr. Frank Baylis:** I don't mean the data that I can see you have collected.

I'll be clear on this question. What I'm talking about is that in your servers in your back offices, you have data on Frank Baylis.

**Mr. Colin McKay:** Yes.

**Mr. Frank Baylis:** It's that data.

I know that you can say “when you collect data here...”, but I'm talking about the data that you don't delete when I say “don't follow me”, the data that you do keep anyway.

For that data that I want removed, can I get that done?

**Mr. Colin McKay:** If you tell us that you want us to delete your account and delete the data associated with it, we do.

**Mr. Frank Baylis:** It's not My Account either....

I want to be very specific here. You have data points on Frank Baylis, and I don't want you to track me at all, not going forward, backwards, sideways.

With regard to the data that you've kept on me, is there any way that I could...? Maybe you don't have the answer now, but could you go and talk to your technical people and ask, “How can I, through a choice, get rid of that?”

**Mr. Colin McKay:** The reason I'm being specific about your account is that it's in that way that we know it's associated with an individual, however they call themselves.

**Mr. Frank Baylis:** I know what My Account is, and I know how I interact with My Account for what I see about what you track on me. There's a difference between what I see that you track on me and what you nonetheless continue to track.

I'm more concerned about what you continue to track regardless of what I say in My Account. That's what I'm asking about.

**Mr. Colin McKay:** I'm trying to be responsive.

The data that we have that we associate with you as an individual is represented in My Account. Your decision to say "stop tracking me and delete this information" is exercised through My Account.

**Mr. Frank Baylis:** I know that. That allows me to know that you've deleted what I see that you've tracked on me. It does not—and you'll correct me if I'm wrong, and you don't need to answer now—force you to delete what you have and continue to collect elsewhere on me in your own servers.

This will specifically lead to my next question that you could look into too.

Over the years, your terms of use have changed. They've done so, in my estimation, to allow you to collect more and more data and to change the manner in which you do and don't collect data and what you do and don't have to delete when you so choose.

Could you give us, and I don't expect you to...a listing of all the times that the terms of use have changed, and how that has specifically enhanced your ability to capture data?

**Mr. Colin McKay:** I can't give you an exact listing today, but my response to your question is that the changes in the terms of service and the privacy policy have been a reflection that our users have asked for more detail in how we collect data, and have asked for more detail in how they can access information about that data and how it's used.

The intent is clarity and transparency.

**Mr. Frank Baylis:** Are you saying you've never changed them to allow you more leeway, that none of the changes that have taken place have given Google more leeway to collect and maintain data?

**Mr. Colin McKay:** There have been changes that have been put in place so that information we shared across Google services...so that we could provide better services to you, but that's been transparently communicated as well.

It's never a question of being duplicitous or trying to conceal the use of data. In fact, the changes have always erred toward being over-descriptive.

**Mr. Frank Baylis:** Could you be specific on the changes that have given you more leeway?

My line of questioning is all to do with how much data you're collecting, when you actually have to delete it—and not simply from My Account but from your own servers—and how your terms of use have evolved to allow you to collect and maintain more data, irrespective of whether I ask that My Account delete it or not.

The last question I have, then, in this round has to do with boomerang routes. Are you familiar that?

● (1155)

**Mr. Colin McKay:** I'm not familiar with the term. No.

**Mr. Frank Baylis:** Say I'm in Toronto, and I want to send another email or something to Toronto. Instead of going through the network in Toronto, it would be routed through the States.

**Mr. Colin McKay:** Okay.

**Mr. Frank Baylis:** You're familiar with that issue, then?

**Mr. Colin McKay:** Yes.

**Mr. Frank Baylis:** Has Google ever put in any contract with any company that they must follow Google's routing? Essentially, when my data goes into the United States, all my data can be taken. I have no rights because I'm not an American citizen.

I have strong concerns that our data is being taken that way. From what I've been reading—and you can correct me if I'm wrong—sometimes Google contractually obligates people to route things through the States so they can collect data.

**Mr. Colin McKay:** I can't speak to specific contracts that have that obligation. I know that there are contracts with our enterprise commercial users that try to stipulate that behaviour with their own data. That's a contract between entities. The underlying principle in that routing is based around the efficiency and the reliability of the network.

**Mr. Frank Baylis:** My concern is—

**Mr. Colin McKay:** It boomerangs so that it's in multiple routes.

**Mr. Frank Baylis:** My concern is about data protection. I'm asking a very specific question. You don't have to give the answer yet. Has Google imposed routing regulations such that it would not necessarily need to go through the States? For example, if I send an email within Toronto to within Toronto, I just need it to go that way. I don't need it to go through Chicago and bounce through Detroit and come back up. It's not efficient, but it's efficient if you want to collect data, because it takes my data to an area where I have no control over it.

I'm asking specifically: has Google put in place contracts that force such routing, that dictate the type of routing?

**The Chair:** Thank you, Mr. Baylis.

Next up is Mr. Kent, for seven minutes.

**Hon. Peter Kent (Thornhill, CPC):** Thank you, Chair, and thank you, Mr. McKay, for joining us again.

Let me say at the beginning that I consider the Google search engine to be the pre-eminent search engine in the world. I used it in my previous life as a journalist in the mid-1990s. I use it every day dozens of times, and I think the benefits of that Google search engine are in many ways invaluable.

In recent days, we have learned that there is a dark side to Google's commitments and policy positions, even in terms of a contradiction between your last appearance here and your appearance today. On May 10, you were asked:

> Has there actually been any data breaches from Google's databases compared to what's happened with Facebook?

You replied as follows:

> Not that we're aware of.

Would you like to correct that now? Were you aware of it at the time? We understand that Google sat for three years with the knowledge that there had been a serious breach of Google's data and that the actions taken earlier in March were simply to close down for fear of comparison with the Facebook breach.

**Mr. Colin McKay:** I think you're talking about the announcement around Google Plus.

● (1200)

**Hon. Peter Kent:** It was Google Plus, yes.

**Mr. Colin McKay:** Earlier this year, at the same time that the Facebook and Cambridge Analytica story came out, we launched an internal process to verify that our APIs and internal data protection processes weren't allowing similar lapses in information sharing.

Through that process, what we discovered is that in Google Plus there was a bug, not a breach. The bug allowed apps that had access to a user's public data—data they had chosen to share on their profile—to access elements of that data that the user hadn't necessarily granted permission to. It also allowed the app to access information that the user had shared with a friend in that same subset of data.

Because Google Plus was designed as a privacy-protective tool, we have very limited logs about what is available in terms of behaviour on Google Plus. We don't keep a record of what our users do on Google Plus. We had a two-week window to evaluate whether or not developers were aware of that bug within the API and that they could access this additional information, whether they had acted on it, and whether any information had been collected. Our internal data protection office reviewed that and could find no evidence that there was an awareness that the bug existed or that the data had been accessed or misused.

Once that had been identified, they then went through the evaluation of harm and whether or not they should notify users that this bug existed and that the potential had existed for this to happen. What they determined was that there was no sign that the information, that bug, had been accessed by developers. There was no sign that any information had been shared in a manner they did not expect. Also, there was really no way to notify developers of how to change their access to data, because as soon as we noticed the bug, we closed it.

Also, in notifying users, neither could we identify a set of users that had been affected by the bug, because there were none in the data available to us. Therefore, we couldn't notify them on any behaviour that would change any possible harm from that bug. That was the rationale behind the decision.

**Hon. Peter Kent:** Let's look now at another member of the Google family, the controversial Sidewalk Labs project with Waterfront Toronto.

Less than a week ago, Ann Cavoukian, who is recognized as a world-leading authority on privacy and vulnerabilities to privacy, resigned as an adviser. She said that the commitment from Sidewalk Labs that personal data would be de-identified in its various projects.... We still don't know much about what those projects may or may not be. She didn't believe that the data would, in fact, be de-identified and that personal data would be protected.

Can you speak to that?

**Mr. Colin McKay:** Unfortunately, I'm here on behalf of Google Canada. Sidewalk is an independent company under Alphabet, so I can't speak to their plans or announcements.

**Hon. Peter Kent:** Certainly, within the same larger company, the ownership of that company you would speak to....

Obviously, there must be similar data protection commitments. Those commitments have been made in Sidewalk Labs, as you've made with us here again today.

**Mr. Colin McKay:** I can't speak to their thought process on how they're identifying data protection in the project they're developing. While we have similar ownership, they are independent, and they're tackling a very different project from what Google Canada undertakes.

**Hon. Peter Kent:** You understand the concern that has been raised at this committee meeting since the Cambridge Analytica, Facebook, AggregateIQ scandal first broke. There's a great deal of discussion about the fact that the so-called data-opolies, the massive tech companies, are mostly American and that their subsidiaries around the world are very often subject to the operating policies of these companies.

I'd come back again to your sister company, Sidewalk Labs. Jim Balsillie, who is no minor player in the rapidly evolving digital world, has called Sidewalk Labs not a smart city. He says,

> It is a colonizing experiment in surveillance capitalism attempting to bulldoze important urban, civic and political issues. Of all the misguided innovation strategies Canada has launched over the past three decades, this purported smart city is not only the dumbest but also the most dangerous.

Surely you must have some corporate comments to a statement like that.

● (1205)

**Mr. Colin McKay:** There's a specific reason that Sidewalk is an independent company with a very different mandate and behaves in a very different way. That's because it operates independently from Google, both on data protection as well as the way it's working through the product development in Toronto.

I don't have an opinion on how Sidewalk is conducting their business. The parallels that exist only exist because there is a broader global conversation around data protection and privacy, as well as development of both urban and rural areas.

**Hon. Peter Kent:** How would Google Canada feel about the creation of legislation to embrace some of the elements of the European Union's general data protection regulations?

**Mr. Colin McKay:** This is something that we covered in my earlier meeting.

From Google's point of view, we've already implemented the steps necessary to be compliant with the general data protection regulations. We have internally gone through the hundreds of years of engineers' time to make that transition.

If you were to make those proposals and legislation, we would participate in that legislative process. We would provide our comments. In the end, we would be looking at a landscape that we are already familiar with and that we already comply with in Europe.

The challenge that is presented in Canada is that the extension of GDPR, to a broad extent, would create greater compliance obligations on smaller and medium-sized businesses. They're already feeling that stress, and not just here in Canada, the United States and Asia, but also in Europe, in terms of understanding their obligations under the GDPR, so that's something to keep in mind.

From our point of view, as I said, it's a broader data protection conversation.

**Hon. Peter Kent:** A year ago, a Facebook executive told this committee that regulation, in fact, would discourage further investment by Facebook in Canada.

Would that be a similar case with Google?

**Mr. Colin McKay:** For us, we're extremely happy with the opportunities that are available in Canada, not just in terms of the business but in terms of growing the engineering teams and making an investment in Canada's innovation ecosystem. Regulatory conversations are nuanced, but we wouldn't make a blanket statement like that.

**The Chair:** Thank you, Mr. Kent.

Next up for seven minutes is Mr. Angus.

**Mr. Charlie Angus (Timmins—James Bay, NDP):** Thank you.

Thank you, Mr. McKay, for coming back.

The Prime Minister, when Sidewalk Labs was announced, did say that he had been discussing this idea of a smart city with Google for a number of years. How did the conversations begin between the Prime Minister's Office and Google about moving forward on a smart-cities initiative?

**Mr. Colin McKay:** I'm not sure. I think those conversations.... He must be referring to the leadership of Alphabet when he referred to Google, and to Alphabet itself. Sidewalk Labs was explicitly built to pursue projects like this.

**Mr. Charlie Angus:** Eric Schmidt has said that Google had been looking for someone to “give us a city” for some time and “to put us in charge”. Would Sidewalk Labs fit that model of a city that Google could be in charge of?

**Mr. Colin McKay:** I heard those comments from Eric Schmidt as well, and I think he was generalizing a broader intent to see how technology could be used to improve and develop an urban area by integrating technology.

**Mr. Charlie Angus:** He also said that for this project to succeed, they would need “substantial forbearances from existing laws and regulations”. I've never seen developers of a waterfront real estate development plan come and say they wanted to be exempt from Canadian law. Given Eric Schmidt's comments, could you tell us what Google would think is important enough to exempt them from law in order to make a smart-cities project go through?

**Mr. Colin McKay:** I can't speak to the details of what Sidewalk Labs is intending. I can make observations around the development of telecommunications in Canada and railway and Internet access where—

**Mr. Charlie Angus:** We're not talking about that. We're talking about Eric Schmidt, founder of Google, who said that for this project to succeed, they expect that this government will exempt them from existing laws and regulations. What would those laws and regulations be? Everyone else has to follow the laws. Why not Google?

**Mr. Colin McKay:** I'm not privy to Sidewalk Labs' plans and conversations, so I can't speak to that.

**Mr. Charlie Angus:** Okay, but this is Eric Schmidt saying this, right?

**Mr. Colin McKay:** I think I read the same newspaper article you read.

He was CEO, not the founder.

● (1210)

**Mr. Charlie Angus:** Sorry. I'm never good with my corporate structure.

I want to ask more about this idea because you talk about transparency. If the Prime Minister had been speaking with Google for a number of years on this plan, was the idea that this would ever be put up to competitive bidding, or was this going to be a project and experiment for Google on the Toronto waterfront?

**Mr. Colin McKay:** Once again, I can't talk to the Prime Minister's process, but I thought that Waterfront Toronto actually had a request for information that was a competitive process.

**Mr. Charlie Angus:** Right now, Toronto real estate is more expensive than Brooklyn's. Sidewalk Labs gets 12 acres of some of the most prime real estate in North America. People will be chomping at the bit for this, yet the request for directions for this project said 40 days. Nobody could compete in a 40-day turnaround to get this, but if Google had long prior conversations, it would suggest that the fix was in. It would be in Google's corporate interest certainly to get access to this major real estate development, would it not?

**Mr. Colin McKay:** You'd have to speak to Waterfront Toronto about how many expressions of interest they had for the RFI.

**Mr. Charlie Angus:** Right, but don't you think that 40 days would be... I mean, you were going to build a smart city. You were going to do high tech. This was going to be something Dan Doctoroff said was going to take 15 or 20 years. Would you think that anybody would put that out for 40 days? It would be kind of ridiculous to think that anybody other than Google would be able to compete, right? I'm trying to get a sense of how these megaprojects are done.

**Mr. Colin McKay:** Unfortunately, I can't speak to what Waterfront Toronto knew or didn't know and what fed into their decision-making process.

**Mr. Charlie Angus:** We certainly had the resignation of Ann Cavoukian, who I think carries a lot of respect. Saadia Muzaffar, who resigned, said that this project shows a "blatant disregard for residents' concerns about data and digital infrastructure. There is nothing innovative about city-building that disenfranchises its residents in insidious ways and robs valuable earnings out of public budgets...."

This does reflect on Google. Do you think there may be a better way of engaging with the public on a project that is this incredibly valuable in terms of real estate but is also a symbol of what Google plans?

**Mr. Colin McKay:** The fact that we're having the conversation today means that it does reflect on Alphabet and the sister companies, including Google. However, from what I've seen as a bystander, Waterfront Toronto and Sidewalk Labs Toronto are engaging publicly on these issues. This is part of that dialogue.

**Mr. Charlie Angus:** When the plan was put forward.... We're talking real estate governance, and I know that's not your area of expertise, but when the plan was brought to the Waterfront Toronto real estate committee, they were made aware that this was not just 12 acres: this was potentially the whole of the Port Lands, an extremely valuable chunk of real estate to turn over. They were given three days to look at this, but when it got to a vote it was presented as a *fait accompli*.

How do we reassure the public that we're doing world-class infrastructure if massive amounts of extremely valuable real estate are being turned over with so little oversight, and Google thanks the Prime Minister, saying that they've been looking for someone to give them a city to be in charge of? Don't you think Google could have done a better job in talking with Sidewalk Labs to ensure that this project was being vetted in a proper manner?

**Mr. Colin McKay:** I'm sorry to be repetitive, but this is a decision-making process by Waterfront Toronto, and the process they followed was under their own control.

**Mr. Charlie Angus:** Apparently they've moved a whole new committee to handle the real estate deals, outside the committee that was raising the flags.

Finally, I'm going to ask about IP.

It says that the contracts for Sidewalk Labs are being structured with consultants and vendors so that Sidewalk, Alphabet and Google will own or will have worldwide royalty-free licence to any IP that's being developed out of this project.

Is that in the public interest, or is it going to be in the interest of Eric Schmidt, Google and Alphabet to have that kind of IP control over anything that's developed out of a public project?

**Mr. Colin McKay:** I saw the same report you did, but I wasn't involved in the process and I haven't seen the documents.

**Mr. Charlie Angus:** Did you ask? You are their Google spokesman. Do you get briefed on this stuff?

**Mr. Colin McKay:** As I said, Sidewalk Toronto is an independent company that is pursuing its own business and working with the government independently.

**Mr. Charlie Angus:** Thank you.

**The Chair:** Thank you, Mr. Angus.

Next up for seven minutes is Mr. Erskine-Smith.

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

You worked for the Privacy Commissioner previously, yes?

● (1215)

**Mr. Colin McKay:** Yes.

**Mr. Nathaniel Erskine-Smith:** What year did you work for the Privacy Commissioner?

**Mr. Colin McKay:** It was from 2007 to 2010.

**Mr. Nathaniel Erskine-Smith:** I guess that was a bit before where I was going. In 2013—and I want to get to some other questions, but this was bugging me and I didn't ask it when you were here last time—when Jennifer Stoddart was the Privacy Commissioner, she made a few key recommendations for reforming PIPEDA. One was requiring that organizations publicly disclose their co-operation in sharing information with governments.

You're not going to have this information today, but subparagraph 7(3)c.1 of PIPEDA states that an organization may disclose to government without the knowledge and consent of an individual that information has been disclosed.

Can you provide to this committee the number of times Google has shared information with the Canadian government without individuals' knowledge and consent, pursuant to this section?

**Mr. Colin McKay:** If you can give me that subparagraph specifically, I'll reply in detail.

We've had a transparency report since well before 2013, and certainly during my time at the Privacy Commissioner's, that makes public the number of times we've been asked for information about our users, and importantly, the number of times we've responded with information, because, whether it's an obligation under PIPEDA or in Europe or elsewhere, we always ensure that there's a valid legal authority for specific information, and then only make available the specific information relevant to a request that's made by government or a law enforcement authority.

**Mr. Nathaniel Erskine-Smith:** You mentioned a requirement in PIPEDA or a requirement elsewhere. Others around the table have talked about the GDPR, and we've obviously heard a lot about it.

You are compliant with the GDPR in the EU, one would presume, just as you're compliant with PIPEDA here. Does that mean that a Canadian who uses Google services receives less privacy protection than any EU citizen using Google services?

**Mr. Colin McKay:** A Canadian receives the data protection and privacy protections that are outlined in Canadian law.

**Mr. Nathaniel Erskine-Smith:** That's what I mean. You're not saying we have to comply with the most stringent rules and therefore we're just going to apply them across the board to everyone; some would argue that you're reducing the stringency of privacy protections. You'd comply with PIPEDA here.

**Mr. Colin McKay:** Let's distinguish between legal compliance and then the protections and services that are accorded to a user.

For legal compliance, we have specific legal obligations in Canada that we need to meet, and that's the framework under which we evaluate requests for information. However, we also have put in place privacy and security protections that meet those expectations globally, which means that as a matter of practice and implementation, users see the strongest privacy and security protections across our services.

**Mr. Nathaniel Erskine-Smith:** That's what I want to get at. Is a Canadian user receiving the same level of privacy protections as an EU citizen?

**Mr. Colin McKay:** Yes.

**Mr. Nathaniel Erskine-Smith:** You mentioned data portability in your comments in passing. We've heard that might be an answer to competition antitrust issues. We've heard that it's certainly a component of the GDPR.

Others coming before us have recently talked about not only portability but interoperability. Would you support a change of law here in Canada to require data portability and interoperability?

**Mr. Colin McKay:** I mentioned the data transfer project in my opening remarks. The data transfer project is a solid attempt to start addressing that challenge.

We've long had both the data liberation front and then data takeout tools that allow our users to export their information so they can be used in a different service. The data transfer project is in concert with Facebook and Microsoft and Twitter and hopefully others. It's to enable you in effect to transfer your information from Google services to another service almost seamlessly.

**Mr. Nathaniel Erskine-Smith:** You're familiar with the Honest Ads Act in the U.S.?

**Mr. Colin McKay:** Yes.

**Mr. Nathaniel Erskine-Smith:** That's probably a pretty limited way of tackling the problem. We've heard other testimony here to suggest that we should go further and that there should be more than just a searchable database, which is now going to be required for elections in some modest fashion, but not for other advertising; we've heard recommendations for real-time ad disclosure about engagement metrics, the number of dollars spent, and the specific criteria by which individuals were targeted.

You have made a number of steps absent of the law requiring you to do so. Google has taken a number of precautions and changed, as you were talking about, third party applications.

Are you looking at providing a real time ad disclosure, or do we have to legislate?

**Mr. Colin McKay:** Do you mean real time ad disclosure to the level of detail you have just described for political advertising?

**Mr. Nathaniel Erskine-Smith:** It wouldn't be just political advertising—

**Mr. Colin McKay:** Okay.

**Mr. Nathaniel Erskine-Smith:** It would absolutely be for political advertising, but perhaps for other advertising as well.

● (1220)

**Mr. Colin McKay:** I think the process is iterative, and it's incredibly complex.

**Mr. Nathaniel Erskine-Smith:** So perhaps legislation is needed.

This is a really tricky problem. When Dr. Ben Scott was before us, he recommended that big publishers.... Google is not categorized as a publisher today and they are not a broadcaster today, so they don't have content control obligations in the same way. We know algorithms have replaced editors to a significant degree.

We heard some testimony that, for example, on YouTube, Google has profited significantly from showing advertising based on Alex Jones and InfoWars videos that Google, in fact, has recommended. They have recommended these videos millions and millions of times.

If that's the case, is Google not in some way then responsible for the misinformation being spread, and shouldn't there be some level of disgorgement then? If you're making money off that misinformation, should it not be disgorged?

**Mr. Colin McKay:** You have pretty clear policies and guidelines in place that we apply to content that's available on YouTube and elsewhere, which we've applied stringently, and we're continuing to tighten the enforcement.

**Mr. Nathaniel Erskine-Smith:** Who flagged that problem for you? YouTube recommended Alex Jones' videos millions of times. Did you finally say, “Oh, we should stop doing this?” Did someone bring it to your attention?

**Mr. Colin McKay:** It's a multisided process. We have automated review. We also have human review. Then we have YouTube users who flag specific content.

**Mr. Nathaniel Erskine-Smith:** You can see, though, that if a company isn't proactively preventing this from happening in the first place, lawmakers like ourselves think we have to fix the problem if the companies are not going to act in the public interest themselves.

**Mr. Colin McKay:** You mentioned a specific person and a specific site. In that instance and in many other instances, there are specific pieces of content that could be found objectionable, yet not violate our policy guidelines or not violate law within a jurisdiction, or there could be. We're trying to balance that law and intervene where necessary, but it's not a yes/no binary option around whether someone has access to our services.

**Mr. Nathaniel Erskine-Smith:** I understand.

This is my last question.

Maybe we need a better process whereby Google's not policing content and not being asked to police content. If Google has profited from hateful content, and you have the engagement metrics to know how many eyeballs have seen it and you have the internal measurement to know how much you have profited through advertising for that content, why should you be allowed to profit from that content? Once it's deemed to be hateful and we know the engagement metrics, pay the money back. Disgorge.

**Mr. Colin McKay:** Ideally the content comes down very quickly, and in fact what happens as soon as we enter into that review process is we stop any revenue generation based on that content. It's not a question of a review process taking too long and the content continuing to accrue revenue on the content; that process stops. Sometimes we actually eliminate compensation for content producers altogether.

**Mr. Nathaniel Erskine-Smith:** If any companies profit over a certain level, there should be some level of penalty, perhaps.

Thanks for listening.

**The Chair:** No worries. You will have time for more questions coming up.

Next up, for five minutes, is Mr. Clement.

**Hon. Tony Clement (Parry Sound—Muskoka, CPC):** Thank you.

Colin, it's good to see you. I'm a little bit of a visitor to this committee, but since I'm here and you're here, I thought we'd proceed on that basis.

You may have covered this at your previous encounter, but I wanted to go through the hacking incidents that have occurred, and particularly what we saw on the U.S. presidential campaign. Maybe you've covered this ground.

I don't even know whether it was Gmail or some other service, but my knowledge of the hack on the Democratic national campaign, the Hillary Clinton campaign, is that it was a kind of sad story.

They had rules and so on, and just one human error—and unless we're all taken over by robots tomorrow, human error is going to continue—created the opportunity for the Russians to gain access to every single email of Hillary Clinton's national campaign director. That was on the basis of a Bitly. In a case like that, what these hackers like to do, if they're phishing or spear phishing, is give you a sense of urgency. If you don't do something right away, if you don't click right away, your credit card is going to be compromised or access to your bank account will be compromised or what have you.

There was a Bitly attached to the email that went to John Podesta. He rationally flipped it to his director of IT in the Hillary Clinton campaign, asking if it was for real, if it was legitimate, which was the right thing to do.

The director of IT in the campaign figured out that this was wrong, it was suspect, and flipped the email back—but he forgot a word. He said, "This is legit" rather than saying, "This is not legit." Then as soon as Podesta saw that, he clicked on the Bitly, and the rest is part of the history books now.

I'm just asking a question. Based on that, we know there is human error. You can have all the systems in the world, but human error does take place. How do we...? Maybe it's a combination of education and better systems, and maybe there's AI involved. I wanted your take on this, because we're all coming up to an election campaign and we're all susceptible to hacks. I'd be very surprised if there were no hacking attempts in the next federal election campaign in Canada.

Let me get your side of this issue.

● (1225)

**Mr. Colin McKay:** This is certainly something that we recognize because of the billions of users we have, particularly starting in Gmail. We've attacked this problem in multiple ways over the years.

To start, in 2010, we were notifying Gmail users that we were seeing attempts to access their account, attempts to try to crack their account by force or to send them spoof emails that would force them to make a decision much like yours. We built on those notifications security protections that now give you a notification if we're seeing an attempt to access your account from an unusual area or an unusual geography, so that if someone outside your normal space or even you while travelling log in to your account from elsewhere, you'll get a notification either on your account or on your phone if you've enabled two-factor authentication. We've forced the implementation of two-factor authentication across most of our products so that someone can't just hack into your account by virtue of having the account name and the password. You now need a physical token of some kind.

However, we also recognize that you can force your way into a system through brute force. Jigsaw, which is an Alphabet company, has developed a service called Shield, which is available to non-profits, political parties, and others, to help them counter denial-of-service attacks, where there is that brute force attempt to cause a security system to fail.

As well, earlier this year we put in advanced privacy protection, particularly for elected officials, so they could put in place security controls that we have within the company that not only require two-factor authentication but also place specific restrictions on unusual log-in attempts and attempts to access information within your Google account services. You are forced to provide additional verification. It's an inconvenience for the user, but it also provides more surety of mind that you have the security protection that allows you to identify those sorts of flagrant attempts.

For the general user, I mentioned Safe Browsing in my remarks. Safe Browsing is developed specifically for that concern. When people have clicked on a link and they use the Chrome browser to go to a page, we can see if that move to a page causes unusual behaviour, such as immediately hitting the back button, trying to leave that page, or shutting down their browser altogether. Over billions and billions of interactions, we can recognize the pages that are generating suspicious or harmful content and are causing our users to behave that way. We then generate an API that we share with Microsoft and Firefox that allows them to flag those URLs as well, so that when you actually click on a link to those pages, you get a red warning box that tells you that it's a security threat and most times will not let you advance to the page. Therefore, we're taking insights from behaviour to try to eliminate the concern as well.

**Hon. Tony Clement:** Are you using AI, then, more and more for security purposes?

**Mr. Colin McKay:** We have that integrated into the systems around our search. Certainly we're using machine learning in our analysis of the behaviours and analysis of the content as well.

**Hon. Tony Clement:** Thank you.

**The Chair:** Next up for five minutes is Monsieur Picard.

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

Let's go back to square one in a very simple way to explain how Google works.

Frankly, I don't remember, but when I purchase a computer, Windows is already on it. I go to the Internet and the first page is Google, so I don't have to subscribe anywhere.

In terms of my access to Google, Google has nothing on me at first, besides my IP address. Is that right?

● (1230)

**Mr. Colin McKay:** At that point, no.

**Mr. Michel Picard:** It does not even have my IP address.

**Mr. Colin McKay:** If you're looking at a Google search page, we actually don't have any information about your behaviour. As soon as you enter a search, we'll have some idea about what you're searching for and your IP address on that device.

**Mr. Michel Picard:** Perfect. I have a first request and I'm looking for golf clubs. I have a list of stores and experts, and all that, so you're already aware of what I'm looking at.

**Mr. Colin McKay:** Yes.

**Mr. Michel Picard:** Let's stay on this very simple version of Google. The only thing you have is that this IP address requested this search, and these are the results. This golf club company needs to send advertising.

**Mr. Colin McKay:** Yes.

**Mr. Michel Picard:** My understanding is that you don't give them my IP address.

**Mr. Colin McKay:** No.

**Mr. Michel Picard:** They give you the product to put on your system and therefore spread it over every IP address you have, but that's not an efficient way to do advertising. Usually those advertising companies, whatever company they are, need to target somehow. In order to target and make sure their investment is well placed in Google, they need a return-on-investment appreciation of this operation. Usually they should put their nose into how you target those IP addresses, to make sure that, for example, they will sell golf clubs only to French-speaking persons, so you need a limited number of IP addresses. They should be involved somewhere in the targeting of the site that will receive the advertising, so they are involved in an operation where they can at least work on these IP addresses. Am I right?

**Mr. Colin McKay:** In the limited description that you're giving, the IP address does have a geography associated with it. It's not very specific.

**Mr. Michel Picard:** No.

**Mr. Colin McKay:** The way that this interaction with an advertiser happens is like this. You make a search. You use specific terms. You may write your search in French or you may write it in Croatian. That helps us identify qualities about the search. We then —

**Mr. Michel Picard:** It is not the fact that Google has done that. My issue is that with this very simplistic version of Google, any third party has access to my IP address because they work with you to target the right place.

**Mr. Colin McKay:** No.

**Mr. Michel Picard:** No?

**Mr. Colin McKay:** No.

Advertisers will says to us, “We want to run a campaign.” Let's say that your local sports shop wants to sell golf clubs this weekend. It says, “We want to deliver ads to people in this geographic space, who search for these terms, at this time, in this language.”

Then we have an auction. We say to all our advertisers, “Here is what is available. Someone is searching within this space for this term under these conditions.” Then they bid on getting that space in the advertising segment.

**Mr. Michel Picard:** Let's expand it to all services that you have for which I put down my name, address, age and all that. Do I understand that it works the same way in every case—that this information is totally reserved for your eyes only?

**Mr. Colin McKay:** Yes.

**Mr. Michel Picard:** Then why bother with transparency? Transparency doesn't change the way you work. Before I didn't know what you did with my data; now I just know what you do with my data. You still do the same thing when you deal with my data; it doesn't change the way you work. You just inform your client that now you're transparent. It doesn't give anything. If I refuse for my data to be exchanged, I may see my service refused then. I won't have access anymore to my service because you need my information as exchange currency for the services you sell to advertising.

**Mr. Colin McKay:** I don't think that's true. Because advertising fuels these free services, we need to deliver advertising. Advertising that is more specific to your needs is more relevant to you, and it is more relevant to the advertisers, as you pointed out. It is more valuable to the advertiser, and we hope it's more valuable to you as well. In effect, it's answering a question and it's answering a need that you've expressed an interest in.

However, you can turn off tracking on your browser. You can turn off location services. You can tell us within your account profile that you don't want us to keep track of your preferences. That will provide less detailed and less precise advertising. Hopefully, it's still useful.

● (1235)

**Mr. Michel Picard:** The thing is then, by default, not accessible, because we wouldn't do that. Everything we do and we talk about.... Why don't we just decide that everything you provide to a company is not accessible and you have to opt in to have more information from a third party company? Therefore, I wouldn't bother about my private information because, by default, it would be inaccessible. Would we put you out of business that way?

**Mr. Colin McKay:** I'm sorry. I don't understand the distinction. If, by default, there's no information collection....

**Mr. Michel Picard:** Google can do nothing with my information, because it's private.

**Mr. Colin McKay:** From our point of view, there needs to be a certain delivery of advertising to support the services. That's what makes the services available to all Canadians, not just to people who can pay subscriptions.

What we try to do is be as transparent as possible. That's why you're seeing so much information that may cause you concern. It is because we're trying to be transparent about what we know about you, as an individual—the information that you shared with us—and then, with regard to an earlier question, be transparent about when and if we share it with anyone else. We don't share it with advertisers, and in the case of law enforcement, we share it under certain conditions. We still behave in our users' interests to protect that information.

The reality is that you can operate using Chrome, Google Maps and most of our services without being identified as an individual and without having a Google account. It will just be a lot simpler, with a lot less detail that's relevant to you as an individual.

**Mr. Michel Picard:** Thank you.

**The Chair:** Thank you, Mr. Picard.

Next up, for another five minutes, is Mr. Kent.

**Hon. Peter Kent:** Thanks very much, Mr. Chair.

Mr. McKay, not long ago the National Research Council warned the Government of Canada that Canada was at risk of becoming a nation of “data cows”, basically leaking or giving away some of our most valuable national resources to companies like yours.

I know that you've separated Google from your sibling company under the Alphabet umbrella with a lack of knowledge. However, surely when people like Ann Cavoukian criticize the mystery, the lack of information and the contradictions of things like de-identifying data or of privacy by design or by consent, you must be concerned—Google must be concerned—on how that reflects on your company and the very similar concerns mirrored by what we're seeing with the Sidewalk Labs controversy.

**Mr. Colin McKay:** I think I can answer to two separate points. You mentioned the NRC's observation about the use of data. I think that observation points to the wrong point in the process of innovation and creation, because data is not scarce and data is not a resource to be conserved; data is in fact readily generated by all sorts of activities and is available in many ways.

The true process of innovation is developing the tools and the services to be able to translate that into products and services. In that observation from that particular document, what's overlooked is how we at Google create tools and services that allow Canadian companies—and others around the world, in the case of TensorFlow—to use the insight from artificial intelligence research to drive product development based on their own datasets. Our artificial intelligence researchers also make available testing sets so that Canadian companies working in that field can evaluate the data available to them and use it more effectively, without involvement or possession or any benefit accruing to us other than using our tools.

On the other element about Sidewalk Labs and privacy, I joined Google from the Office of the Privacy Commissioner because there was already a path of deep introspection and product development on data protection and privacy. That has continued, and it's continuing apace. Through the changes I told you about this morning and in more to come, we're focusing on improving privacy and data protection for our users.

We've been in healthy conversations with Dr. Cavoukian in the past on these elements. As a company, we see ourselves pursuing a strong conversation around data protection and its evolution, whether within the context of civil society or commercial use. Sidewalk Labs is following one path, and we're following another. We have the resources available to put in place the protections I've described today.

● (1240)

**Hon. Peter Kent:** Has the Privacy Commissioner of Canada been in contact with you or with Google as part of his investigation of the Cambridge Analytica-Facebook-AggregateIQ scandal?

**Mr. Colin McKay:** Not that I know of.

**Hon. Peter Kent:** All right.

How do you respond to reports such as the one from the Associated Press, which I think said that despite Google's statements, such as your statements here today about not following users when they request that Google make the break, in fact Google does continue to track users even when they don't consent to being tracked?

Is it a splitting of hairs that when people give the blind consent that we know many of them give when they accept conditions, they don't realize that this consent includes being tracked and having their data accumulated?

**Mr. Colin McKay:** I think I run the risk of your accusing me of splitting hairs, but realistically, we provide a control within your account on location tracking.

The reality of using mobile phones within a mobile network is that your mobile phone is constantly sending a signal about its location to the network. That data is available in a separate track, and we can only speak to how location data is being used within our network, within our constraints. If others are using the data that's being shared with the cellphone network, then that's something that I can't speak to, but there is a reality there.

As we discussed in May and again today, for the user, the interaction is often complex and the clarity is not evident. In that case, it needs to be further clarified.

**The Chair:** Okay. Thank you, Mr. Kent.

Just before we finish the round, we're going to let it go again. If there are any questions, they can be asked. We have until one o'clock. We also have some committee business at the very end for about 10 minutes.

Mr. Angus, you have three minutes.

**Mr. Charlie Angus:** Thank you very much.

I had the pleasure a number years back of meeting with employees at Google in New York. I have to say that in terms of a corporate structure, you have hired the best of the best, people I think are brilliant, people with a sense of a vision of where they need to go. I just want to have on the record how much I respect the employees at Google.

We saw recently that it has been employees at Google who have been challenging certain corporate decisions that are being made—for example, in Project Maven, which was the facial recognition project with the Pentagon for drones. People were not willing to participate in that project because they didn't feel it reflected the culture that Google was founded in.

Recently 1,400 Google employees signed a letter to raise deep concerns about Project Dragonfly in China, regarding the question of capitulating to the censorship and surveillance demands in exchange for access to the Chinese market. The letter says that it's a forfeiture of our values to go along with this project.

In the United States, we've been told that Google management has ordered that memo to be taken down. Have there been any steps in Google Canada to stop employees from speaking up about Project Dragonfly?

**Mr. Colin McKay:** I will address that with a general observation first.

I take great pride in the fact that I work at a company, as you've observed, in which employees are allowed to voice their opinions, including opinions about product strategy and company strategy. As you pointed out, product decisions are made by the senior leadership of the organization.

You mentioned Project Maven earlier. Project Maven, as it applies to the implementation of artificial intelligence, was part of the conversation around the development of our principles for the use of artificial intelligence, which was a collaborative effort across our engineering and product teams and leadership to clearly communicate how we were going to approach the development and implementation of AI.

With respect to the specific question you asked, there hasn't been direction like that in Canada.

**Mr. Charlie Angus:** I'm looking at the letter that was signed by Google employees. They were very concerned about capitulating to China in terms of setting up a search engine that would allow dissidents to be tracked. They said, "...we have not made clear what our red lines are in this area internationally."

I raise this because one of the things that made Google such an exciting company when it was formed was that it had a policy of doing no evil, and it decided to drop that model. Now we see these deals with the Pentagon and the Government of China.

From a regulatory point of view, it's rather disturbing that a company with as much power as Google can make these decisions in the face of its own corporate culture, about which its employees are speaking up.

What do you think we should be looking at in terms of regulator oversight to make sure Google is not doing evil?

● (1245)

**Mr. Colin McKay:** We demonstrate through action, whether through the principles on AI or our transparency report, what our interactions are in a concrete and demonstrable way with those governments and what our intent is with products. We've moved on from a world where we had a very simple suite of products into one where we're pushing innovation and service delivery across a number of areas. That communication becomes more complex, but we continue to have that internal dialogue.

**Mr. Charlie Angus:** When you came here in May, we asked if there had been any data breaches, and you said you were not aware of any, yet in response to Cambridge Analytica, you said you had done this analysis of Google Chrome's data breach, and that had been flagged. The Wall Street Journal said that the decision had been made not to disclose this breach last spring partly because of fears that it would draw regulatory scrutiny.

Here we are, a parliamentary committee, and you came to tell us there had been no data breaches. Were you aware of that, or did Google's head office just not tell you there was a data breach that should have been disclosed to our committee when we invited you the first time?

**Mr. Colin McKay:** I think you're referring to the Google+ item that we discussed.

**Mr. Charlie Angus:** Yes.

**Mr. Colin McKay:** That was not a data breach. That was bug.

**Mr. Charlie Angus:** I'm not a tech guy, but I can read. Google said it was worried it would draw regulatory scrutiny. You came to our committee and told us everything was fine. Google knew things weren't fine. The question was about regulatory scrutiny. Were you made aware of that when you came here, or were you just splitting hairs and weren't telling us that?

**Mr. Colin McKay:** I was not aware of it when I appeared, and our evaluation determined that it was not a breach; it was a bug.

**Mr. Charlie Angus:** But you were worried about regulatory scrutiny.

**Mr. Colin McKay:** I can't speak for the authors of that memo.

**Mr. Charlie Angus:** Thank you.

**The Chair:** It looks like we have one more question from each party, so we'll start off with Ms. Vandenbeld and then go to Mr. Kent and Mr. Angus. We should be done then, but we'll see where the time goes.

Goahead, Ms. Vandenbeld.

**Ms. Anita Vandenbeld (Ottawa West—Nepean, Lib.):** Thank you very much.

I'd like to go back to the part that you discussed in the beginning when you outlined the key areas on controls, particularly, in this case, not the Google search engine but YouTube. Obviously certain things on YouTube that would go against the user policy are automatically removed, or the person is informed that it's been removed because they're violating the policy.

I would be very interested in knowing how those determinations are made. For instance, is it an individual person who looks at those? Is it an algorithm? Are you using some sort of AI? Are there keywords that you're looking at?

There are a couple of things that I'm a bit concerned about. After the testimony at this committee of Mr. Vickery, I posted my questions back and forth, just like you and I are doing right now. It's televised; it's on ParlVu. One of the questions that I asked was about the fact that some of this data had been found on a Google drive. When I went to post that intervention, which was from a parliamentary television site, it was found to violate the YouTube.... The only caption was the name of our study, which is the breach of personal information involving Cambridge Analytica and Facebook. It was removed, and I was told that I would have penalties. I went for a review, and of course, after a review it was posted back on again.

I know of another member of Parliament who asked a question in question period about cannabis, and that was removed because it was said that he was promoting the use of drugs.

How are these determinations made? What are the algorithms or terms, or how do you do that with YouTube? There are, at the same time, an awful lot of things on YouTube that promote hate, that are anti-democratic, that are perhaps even put there by interests that have links to international crime.

I worry that the way these algorithms are being used might not necessarily be capturing what we really want to remove, while free speech in an environment like this, which is a parliamentary committee, has been actually caught in this net.

● (1250)

**Mr. Colin McKay:** You're describing two very specific cases that I'll dive into right after an observation.

We have intensive review processes that are driven by algorithmic decision-making as well as a focus on keywords, and then also details about the account itself. For example, on a brand new account attempting to post content on flagged material, you may see that you're not able to post it publicly before it's reviewed. You may see that you're not able to monetize it until we've actually reviewed it. We go through this process to ensure that we're checking it against the corpus of material that we are aware of.

I say that specifically because in your first instance, it's quite possible that when you posted a video of televised CPAC material.... CPAC has worked with us to register CPAC material as material that needs to be reviewed under our content ID guidelines. That's our protection for copyright holders that want to avoid television programs, movies, music from being posted by users without their permission.

**Ms. Anita Vandenbeld:** It's a very common thing, CPAC. I've posted things from committees all the time.

**Mr. Colin McKay:** That's my supposition as to why that happened.

**Ms. Anita Vandenbeld:** That wasn't the reason given.

**Mr. Colin McKay:** Okay. I didn't have that information.

On the cannabis example, there's a relatively fast-breaking space here, and we're trying to adjust our internal systems to differentiate between the promotion and use of cannabis in the illegal context, especially in an international arena, versus what's happening in Canada and the fact that it's now legal. With our advertising systems, as you might imagine, we're learning internally, through that algorithm, through manual review, through flagging by our users, that there's certain content that is now allowed and certain content that isn't.

It's an iterative process and it overlaps technology and human intervention, and that's especially important in sensitive areas. What happens in the case of violent content or extremist content is that once we're given an opportunity to recognize that there's a video or audio clip that is objectionable and illegal, we can use that same content ID flagging system to identify it as soon as it's uploaded and make it unavailable, and in some instances we shut down that account.

**Ms. Anita Vandenbeld:** How many resources do you have in terms of actual people who are able to review this material? How much of this is just done automatically by algorithms—

**Mr. Colin McKay:** Hundreds.

**Ms. Anita Vandenbeld:** —and how much is it actually...? Do you have sufficient resources—

**Mr. Colin McKay:** I can get you a full number, but it's a continuing level of investment, both on a technological basis and a human basis, to provide the review.

**Ms. Anita Vandenbeld:** Thank you.

I will give the questions to Mr. Erskine-Smith if he wants them.

**Mr. Nathaniel Erskine-Smith:** I just have one question.

There were two topics that I failed to cover. One is algorithmic transparency. We've had witnesses come before us and say there need to be third party auditors who step into Google's offices and Facebook's offices and assess whether the algorithms you're employing are being used in an appropriate way. Would you have any problem with that?

**Mr. Colin McKay:** To me, that's looking at the wrong end of the processes, because in many cases that have been identified so far, it's the data that has demonstrated bias. If you're running an algorithm against biased data or an unrepresentative sample, then you're going to get erroneous or erratic results.

In some cases the algorithm is proprietary commercial technology, and I don't know if an auditor would have the capacity to evaluate what the algorithm is intended to do, or how they would evaluate working versus non-working and under what standard.

**Mr. Nathaniel Erskine-Smith:** Potentially, then, it's a practical problem for us to solve, but in theory there's not necessarily an objection.

The last thing is just on regulating speech. The right to be forgotten, potential privacy towards defamation, harassment, hate.... There are reasons for material to be taken down.

Do you have a preferred model of how this information should be taken down? If Google doesn't want to be the police, who should be? Should Google pay into a fund to have a public body administering and making these decisions? Do you have a view as to how this should work?

**Mr. Colin McKay:** I'll just make one observation before I answer, because you mentioned the right to be forgotten.

There's an ongoing conversation around the right to be forgotten in Canada. One thing the Privacy Commissioner highlighted in his consultation document and his guidelines was that there's an inherent conflict with the charter on freedom of expression and that there needs to be a full-throated conversation in public, ideally at this committee, around how the right to be forgotten should be exercised in Canada.

From our point of view, these processes exist. They're called the courts. The courts have an understanding of both the standards and the public expectations. They have the tools available to them to—

● (1255)

**Mr. Nathaniel Erskine-Smith:** We can't expect the courts to take down content all the time, though. There are so many pieces of content that should be taken down. You can't expect someone to pay a lawyer like me $400 an hour to run off to court and take down a little comment here and a little comment there. What would be a better system?

**Mr. Colin McKay:** The alternative that you're describing to me is the process that exists in Europe, where you ask us to make an evaluation about whether your protected expression violates—

**Mr. Nathaniel Erskine-Smith:** Does it cost too much? Doesn't Google make enough to pay for it?

**Mr. Colin McKay:** —a fundamental charter right, and then you are giving us the responsibility of an administrative court. The question is whether you want to do that or not.

**The Chair:** We have a couple of minutes left. If we can divide that up, it would be great.

**Hon. Peter Kent:** I have one very quick question.

Fortune magazine tells us that Google outspent every other company in North America last year in lobbying Washington. I'd like to know how much Google has spent in Canada lobbying governments at the federal, provincial and municipal level, and how many registered lobbyists you have in Canada.

**Mr. Colin McKay:** We have three registered lobbyists. That's my team. They work here in Ottawa. I can't give you the exact expenditures. They're not sizeable. What we do with that lobbying is this sort of interaction, whether on an individual level or at committee or with broader society. The reality of that number is that we are trying to be transparent about our interaction on what is obviously an increasingly complex set of subjects.

**Hon. Peter Kent:** Would Google Canada separate its lobbying efforts from those of Sidewalk Labs?

**Mr. Colin McKay:** Yes.

**The Chair:** Go ahead, Mr. Angus, for one minute.

**Mr. Charlie Angus:** Very quickly, I'm just following up on the question of lobbying, because of a question of this government's relationship with the data lobbyists—and there's nothing wrong with lobbyists.

John Brodhead was very involved with the Liberal government. He was in infrastructure, and he helped write the platform. Now he's the point person for Sidewalk Labs.

Prior to his being appointed to Sidewalk Labs or hired by your sister company, did any of the Google lobbyists meet with him?

**Mr. Colin McKay:** I believe we met with the department of infrastructure to talk about transit investments between Toronto and Waterloo.

**Mr. Charlie Angus:** Right. That's it?

**Mr. Colin McKay:** Yes.

**The Chair:** Thanks to Google and Colin again for coming to our committee.

We're going to forgo our committee business. We've made a decision about Thursday. We have the Dutch PM coming to speak, so we're not going to have committee on Thursday, where Facebook would have appeared. We're going to push that to another day.

Thank you for your testimony and for taking questions. Have a good day.

The meeting is adjourned.