HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 053 • 1st SESSION • 41st PARLIAMENT

EVIDENCE

Tuesday, October 30, 2012

Chair

Mr. Pierre-Luc Dusseault

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, October 30, 2012

● (1530)

[*Translation*]

The Chair (Mr. Pierre-Luc Dusseault (Sherbrooke, NDP)): Order, please. It's 3:30, so we'll start the meeting.

As per the agenda, we are continuing with our study on privacy and social media. We have with us today Colin McKay from Google.

We'll proceed in the usual manner and start with a 10- or 15-minute presentation. As the only witness, you can have a bit more time. That's no problem.

Then we'll move on to questions and answers for an hour or an hour and fifteen minutes, depending on the questions. If there are still questions after that, we can carry on with the meeting. I'm at the committee's service. We'll see how things go.

Without further ado, I'll hand the floor over to Mr. McKay.

[*English*]

Mr. Colin McKay (Policy Manager, Google Canada, Google Inc.): *Merci*. Thank you, Mr. Chair, members of the committee.

My name is Colin McKay. I'm a policy manager working for Google Canada. Thank you for inviting me today and for giving me an opportunity to talk a bit about Google, and in particular, Google's policies on privacy protection and user control of personal data.

Canada is important to Google. We have offices in Kitchener–Waterloo, Toronto, Montreal, and Ottawa. Our engineering offices in Montreal and Kitchener–Waterloo are growing particularly quickly. These offices are developing products that are being used by hundreds of millions of people every day worldwide. Particularly relevant to today's meeting, our Montreal office works on products that make your online experience as secure as possible, and for users around the world.

Google Canada has also been working to help small business owners across the country use the Internet effectively to grow and flourish. To recognize their success, we created the Google eTown awards, which are designed to showcase communities that are leading the way by using online tools and services.

We looked at countless cities and towns across Canada and found that some municipalities—Moncton, New Brunswick; Dorval, Quebec; Parry Sound, Ontario; Canmore, Alberta; and Duncan, B. C.—stood out from the crowd. They exhibited strong engagement and potential for growth within the digital economy.

Google is proud to help Canadians not only make the best use of the Internet, but also to help them do it safely and securely.

Privacy and security matter to us, and we know how important they are to users. It's what our users expect from us and it's what we expect from ourselves.

That's why we at Google are committed to the highest security and privacy standards. We've backed up our commitment with real dollars and people. We spend hundreds of millions of dollars every year on security, and employ world-renowned experts in data security, who work around the clock to keep your and my information safe. We provide a whole suite of security and privacy tools so that individual Canadians can take control of their data management in a simple and straightforward way. With a few clicks of the mouse, users can remove all of their web history from Google's records, and at the same time, if they choose, prevent Google from recording their web history in the future.

We also provide Canadians with tools to secure their information while using the web. Two-step verification for Google accounts provides each user with extra protection against unauthorized access to their information. Our Chrome browser, which is increasingly popular among users around the world, includes something called the “incognito mode”, which allows a user to browse the Internet in what we can call “stealth mode”. Any pages opened or files downloaded aren't recorded in Chrome's browsing or download history. This is especially useful for users who regularly access the web on public computers at libraries or cafés, which are renowned for being large security holes. They're also useful if you're planning a surprise party and you just don't want your family members to stumble across something that you would rather keep a secret till a future date.

We strongly believe in data-driven innovation at Google. It's the kind of innovation that leads to things like crisis maps, developed on the fly, that help forecast the impact of hurricanes like Hurricane Sandy, or the creation of more pedestrian, yet extremely useful services that help you plan your vacation more quickly and more cheaply. We are constantly improving our products and creating new ones using a variety of data sources. Much of this data is pulled from other sources, but some of it is provided by users.

Data-driven innovation at Google also means developing and improving our security mechanisms and processes, meaning we use data to protect our users and the web at large.

When you get right down to it, I think we can all recognize that while providing user control is important, without strong security to keep data safe, it's all for naught. So before I discuss how we enable users to control their data, I'd like to start with a few examples of how we keep that data safe.

All 425 million active Gmail users, and the people in contact with them, receive extensive protection against spam, phishing, and malware every day.

I suspect there are some Gmail users in the room right now. I'd just prompt you to think about the last time you actually saw a spam message in your Gmail inbox, as opposed to any of the other services I'm sure you'd choose or are forced to use.

● (1535)

We have built-in encryption to protect messages from snooping by others, such as when you use your laptop at a coffee shop. Session-wide secure socket layer encryption is the default not only when you're signed into Gmail, but also Google Search, Google Docs, and many other of our services. We provide end-to-end security for your communication when you're using our services online.

Our ability to analyze search logs, which are aggregated sets of data, helps us identify and reduce vast amounts of web spam. This data has also helped lead to the creation of what we now consider indispensable search features like autocomplete, Google Instant, and spelling correction.

If you just pause for a few minutes and try to remember what your search experience was like in 2006, 2004, or—forbid—1999, you'll remember it was a much more difficult process trying to iterate how you misspelled words to get an accurate answer. Nowadays Google Search just delivers something instantaneously, based on analysis of these logs and past behaviour.

The analysis of aggregate data has also helped us create Google's Safe Browsing technology. Every day, engineers at Google examine billions of URLs, looking for sites that are dangerous for anyone using the Internet. This can include malware sites that contain malicious code intended to force-install keyloggers on your computer and other crimeware and phishing sites that masquerade as legitimate sites, seeking to trick users into typing in their user name and password, for example, something I think we are all familiar with, a site pretending to be your bank.

Because we want to help protect all Internet users and not just those using Google services, we make this security data available to anyone. Apple uses this data to protect users of their Safari browser, as does Firefox for its users.

We know the technology can be complicated. In addition to ensuring the safety of user information, we strive to create user-focused controls and experiences that make it easy to make informed choices about what and how to share your information with us and with others.

Google Dashboard is a tool that can help answer the question: what does Google know about me? Dashboard shows each user the information stored in their Google account. From one central location, you can easily change the settings for any Google services you may use, such as Blogger, Calendar, Docs, Gmail, Google+, and more.

Another great example of user-focused controls is Google+. Through Google+, which is our social network, you have full control over who gets access to different aspects of your presence online.

We all know that the difference between family, friends, acquaintances, and strangers is crucial, especially on a social network. Google+ circles mimic the way we think about sharing information offline to help manage our friends and contacts while online. I could put friends in one circle, family members in another, and a boss or a nosy neighbour in a circle all by themselves. I can then share relevant content, like Google+ posts, YouTube videos, or local listings with the circles I choose.

We've even built some extra protections for youth that encourage safe online behaviour. Posting something for everyone to see on a social network is an especially big deal for young people, so when teens try to share outside their circles we put in an extra confirmation step that encourages them to think before they post. We have also built default protections that block strangers from directly contacting or even saying hello to teens without a teen's express permission.

Another great example of user control is a Google service that I'm sure most members of this committee have used. In fact, most Canadians have used it: Google Maps. The most basic functionality in our mapping service lets you look at a map of your neighbourhood, your city, your region, or any region on earth, wherever you choose to look, but Google can also provide turn-by-turn, real-time directions with the GPS navigation mode in maps. We can help users find places of interest, like restaurants, gas stations, and automatic teller machines.

We could tell a user how long it will take to get to a destination, a particularly useful feature for anyone with a difficult daily commute. In fact, Google can help users bypass a particularly tough commute by looking at aggregated and anonymized historic and current traffic data to find a quicker route home. We can even give users bicycle-specific directions based on data about bike lanes, paths, streets, and even elevation.

● (1540)

I have to admit that, despite our best efforts, users sometimes decide they want to stop using Google and want to take their data with them. We've developed Google Takeout just for this purpose. Takeout makes it extremely easy for users to export the data from many of our most popular services—and we're adding more every month.

We make it easy for users to leave and choose another service, which keeps us honest. Our users are safe and secure with us, but they also don't have to feel locked in.

In conclusion, I've tried to provide the committee today with an overview of Google's privacy and security policies and how they are implemented in practice in our products.

As part of my job, I meet regularly with privacy commissioners to hear their concerns and to work together to develop solutions to any issues that might arise in those conversations.

Google has worked hard to build a positive and productive relationship with Canada's privacy commissioners, both at the federal and provincial levels. This collaborative approach has worked well, by serving as a forum to hear the privacy community's concerns and to help us explain how our business helps Canadians on a daily basis.

Thank you for your time this afternoon. I would be pleased to answer any questions you might have.

[*Translation*]

The Chair: Thank you very much.

Now we'll go right into questions and answers.

Mr. Angus, you have seven minutes.

[*English*]

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

Thank you, Mr. McKay, for coming. I'm really pleased that Google is participating in this study. The overall frame of the discussion that we're having here is that we see the incredible potential for new media: the innovation, how it's transformative, democracy, innovation arts, everything. That being said, the risks, if data is breached, are also enormous. We're playing in a whole different game and you are the biggest player on the field. So what Google does has a huge impact.

I would like to say at the beginning that I was interested in your comments on Gmail. I've never seen spam on Gmail. I've left other services and I've even seen our extraordinarily good House of Commons spam has gotten through on our private servers in a way that I've never seen it on Gmail. So I was impressed with that.

I also want to compliment you on Google+. I think the idea of the separate circles is huge. I know many young people in my riding befriend me as their MP, and sometimes I want to check to see who they are, and I'm seeing all kinds of high school conversations that I really don't believe I should be seeing, but it's out there. If they had a Google+ system perhaps....

Again, it might be a case of Beta versus the VHS right now in terms of new media. So I encourage you...but you don't have the market share.

I guess I'd like to start by asking you about some of the breaches that we've seen, because when the breaches happen they're enormous. The FTC levied a $22.5-million fine for the breaches on Safari, in getting around the Apple cookies.

What was that about? And what have you done to address it?

● (1545)

Mr. Colin McKay: I will first start by thanking you for your comments about Google+ and Gmail and for recognizing the connection between privacy and security. It's a point that I stated quite repeatedly in my comments, but I think it's an important one.

Speaking specifically to Safari, there are two separate issues between the FTC's judgment on Safari and then, separately, the technical issue around the cookies. We made a mistake and we've corrected it and we've moved on from that. The mistake was made in the effort of providing services to our users that they had indicated they wanted.

There's a technical explanation about what happened with the cookies, which I would be happy to explain in a little more detail. I just don't think this is the place to do it.

Mr. Charlie Angus: I wouldn't understand it anyway.

Voices: Oh, oh!

Mr. Charlie Angus: Mr. Calkins might, in his line of questions.

Mr. Colin McKay: What I would underline is that in this case it was a mistake, and it was made with the best intentions. We recognized that it could be misinterpreted. We've corrected those mistakes.

Mr. Charlie Angus: I guess there's the question of mistakes, when on July 27, with the U.K., there was the issue in terms of the amount of 600 gigabytes of data that had just been picked up in the wireless Street View. I mean, Street View went through...and information off wireless networks, that's....

For an outsider, it showed us the incredible ease it takes for an organization as powerful as Google to just pick up whatever kind of information it wants. So we have to trust on your "do no harm" principle, but mistakes like that could have an enormous impact. That's people's banking data, privacy data, and to see that it was just picked up so easily, and then that it wasn't erased....

What steps do you have in place to assure the public that you're not Big Brother?

Mr. Colin McKay: I would say we're certainly not Big Brother. We have the users' interests in mind. We're providing security controls for them that allow them to control their information. That analogy, I think, would be reversed in that we're providing them services that ideally provide them with very secure communication products.

I'm in a difficult position when it comes to WiFi. When I left my previous employer, the Office of the Privacy Commissioner, I was asked to not deal with any ongoing files, and WiFi was the one file. I'm afraid that I'd have to get back to you about speaking to particulars about WiFi. I don't mean to be evasive, it's just the one file.

What I can say to you, though, is it's not in our best interest to blindly look for information. We're looking to improve services and provide products for users. That's our main goal. That's reacting to the two examples you've brought up. That's why we've made incredible investments in the privacy and security teams within the company, to make sure we have internal processes in place to avoid those sorts of problems in the future.

Mr. Charlie Angus: Well, that's excellent. I won't put you on the spot there. Perhaps you could have someone from Google—

Mr. Colin McKay: Yes.

Mr. Charlie Angus: On this issue of the 600 gigabytes of data, I mean, that's a big question mark out there, and it's certainly something we've pondered. If we could get an explanation, that would be helpful.

I'm interested in this as well. Going back to the European Union, on March 1, they were saying you're not in compliance with European Union law on privacy. I'd just like to look at it, not so much with the specifics of the EU, but on the larger philosophical question we've been wrestling with. We want to encourage innovation. We know the Internet is an international tool. We know that for you to have a business model that works, you have to be able to run a platform all around the world.

In terms of compliance with privacy laws, we have our privacy laws in Canada, which we're very proud of. The United States has a different standard. The European Union has a different standard. How does Google find a way to maintain a service that not only works all over the world, but also is in compliance? Are you that far apart from the EU standard, or do you need to rethink your business model?

Mr. Colin McKay: We believe we're in compliance with European law. We've also made investments in staff around the world—people like me—to make sure we're aware of where data protection and privacy law is moving on a country-by-country basis so that we continue to be in compliance around the world. That's the effort we're making so that we can meet the expectations of our users in every country.

What I would say about legislation in Canada is that we see Canada as having a particularly interesting and useful privacy framework. It allows us to have conversations with the Privacy Commissioner about upcoming products and services so that we can have an open dialogue and record their impressions about what we plan to do and what we plan to launch in the market, and try to reflect that in what we eventually provide to Canadians.

● (1550)

Mr. Charlie Angus: Just quickly, I have a question on the issue of Google Takeout. We've talked a lot about the right to be forgotten, the whole “do not track”, that if a citizen wants to pull out they should be able to pull out. We haven't seen any real mechanisms of how possible that is.

You're telling us that you have a system in place. Can you explain that to us?

Mr. Colin McKay: It's just that: it's a system. If a Google user decides they want to withdraw from all our services and they want to take the information they've shared with us, we're building a mechanism so that product by product, with one simple button, they can not only pull that information out of our systems, they can send us a signal they want that deleted. We'll provide it to them in a format that they can then use in an alternative system. That doesn't necessarily mean service to service, but it means we won't give them some unintelligible electronic file that they can't analyze.

The goal really is to keep us honest and to provide our users with a tool that allows them to make that clear decision about whether or not we're providing value and usefulness to them on a daily basis.

[*Translation*]

The Chair: Thank you.

Mr. Angus, your time is up.

It is now Mr. Calkins' turn.

[*English*]

Mr. Blaine Calkins (Wetaskiwin, CPC): Thanks, Mr. McKay, for being here.

I might have a little bit of insight on some of the more technical aspects, but I don't think we need the conversation to go there.

I have some questions for you straight up front. You talked about Google Chrome and you talked about how it has that incognito mode. Then immediately you proceeded to talk about analyzing search logs.

When you're talking about Google Chrome, I mean, I'm going to make a fairly broad assumption here. Google's corporate worth comes from its data. Your most strategic asset is your data. That's mostly user data, user trends. It's what makes you marketable.

Now, you're selling it to me today, at committee, and I believe you. I believe strategically that it's in Google's best interest to provide the best service possible for its customers. But I'm not your only customer. I'm a user of the Google product. Your customers would be any other marketing agency that might want to have access to what my preferences might be, what my trends might be, what my shopping interests might be. That's based on my navigation and browsing history.

So when you talk about Google Chrome not having anything tracked or preventing history from being loaded, you're simply talking about on the local machine. You'll still know where I've been, because that will be tracked elsewhere. Is that not true?

Mr. Colin McKay: Let me start off by saying, to one point in your question, that we don't sell data. We don't sell data to third parties.

Mr. Blaine Calkins: Okay. Fair enough.

It's not selling data, but you would sell information, or you would give broad marketing indications to people, right?

Mr. Colin McKay: We provide advertising services based on some of the data, but let me make the distinction—

Mr. Blaine Calkins: But it's user-specific advertising, right?

I mean, it's evolved, and I know it's evolved, because I get ads on my browser that are specific to, you know....

I'm a hunter, and I go to hunting sites and fishing sites, so I get stuff from Bass Pro. I get all kinds of stuff all the time. That's not a surprise. I know how it works. That's fine. I appreciate it. This isn't meant as a criticism, and I'm not going on attack mode here.

I am concerned simply about the privacy aspect of it. I've been a database administrator. I've looked after millions of dollars' worth of financial transactions. It's been my responsibility to look after data. I'm pretty sure about what I'm talking about. But I've never done it in a social media context. Everything I've done has been private, financial transactions and whatever the case might be in a corporate setting. I understand what you're doing here.

My issue is that I've got constituents who are also users of your services who would have legitimate concerns about their privacy. If you want to talk about the technical aspect of cookies and how those things are tracking.... I know what a cookie is; I know what a secure socket layer is; I know what SSL technology is. I know these things.

So when we're talking about local versus centralized, you would be gathering the data on me as a user. Just because you're not tracking a cookie on my machine, or putting a cookie or a log history in, you would be able to know if I logged into any of my Google accounts. If I were logged into Gmail or if I were logged into anything, you would be able to record that browsing history, not maybe to the infinitesimal point where that data is being stored with my name associated to it in your database. That's where the value comes from your data collection, is it not?

Mr. Colin McKay: Let me make three separate distinctions.

To answer your last question, if you're in incognito mode, you're completely anonymous to us. You're using the service in, to use the vernacular, the dumbest format possible. It does not provide tracking or customization; it provides you with a very clear browsing history that is not recorded.

● (1555)

Mr. Blaine Calkins: Locally.

Mr. Colin McKay: No: completely.

Mr. Blaine Calkins: Completely.

Mr. Colin McKay: Completely. Incognito is your anonymous way of accessing the Internet.

The other two distinctions I would make are these. I was careful in my comments to make the point about anonymized and aggregated data. As you discussed what data may or may not be valuable to the company, I was careful to emphasize that there's a substantial amount of what could be classified “transactional” or “network” data. This is about how traffic is being communicated through the network and how we see attacks on customers' accounts. That isn't necessarily user data but it is relevant to a user. We find that data very valuable, and that's what allows us to provide security services not only to the individual but to our whole company and the Internet as a whole.

There is a vast quantity of information that's not specifically user data. It is still extremely valuable to the company because we use it to turn around and provide services to individuals that allow them to operate more safely and securely and to have greater access over their own personal information online.

Mr. Blaine Calkins: If people were to log on for the very first time, download Google Chrome, and start using it as a user, they would never get any targeted, specific advertising based on their browsing history, because if they stayed in the incognito mode you would have no idea who they are? Do I understand that correctly?

Mr. Colin McKay: Yes.

Mr. Blaine Calkins: That's a great answer.

I want to talk a little bit about the delete versus.... I have a Gmail account so on. Notwithstanding how frustrated I am when I download third party software that asks me if I want to install the Google tool bar on my browser—which I don't, because I don't want to be tracked, and I don't want to have that there—at least I have the option to check it off, even though the default is to include it.

We've had lots of testimony from witnesses here about the devil being in the defaults, when it comes to the big blanket privacy policy statement in which people have to accept everything. I don't pay for any Google services; I get it all for free, but that comes at a cost to me because I have to give you something that you can turn around and make some money with. That's how business works; it's not a criticism.

If I wanted to delete my Gmail account—and I think Mr. Angus talked about this—how can I be reassured? You talked about providing the information back to me, and I could port over to another platform if I wanted to leave the Google platform, say, and move to another platform for my search engine or whatever the case might be, my e-mail client.

How can I be reassured that this is a true delete from your system? Obviously, we can talk about backups, checkpoints, and so on. At a certain point in time I can press that magic delete button, but I'm going to be in your system's history. If you have a system crash and restore it to a certain checkpoint, I might get put back in.

How do you guys manage situations like that?

Mr. Colin McKay: In very general terms, when you go to Takeout and you indicate that you want to export, in this case your Gmail data, and you press that button, we deliver it to you in a format that's accessible for the other products. We also then send a signal to switch the bit, so to speak, so that information is no longer accessible.

Mr. Blaine Calkins: Switching the bit is deactivating, though, not deleting.

Mr. Colin McKay: No, but for us switching the bit means deactivating and then it's no longer accessible, and then that signals the space is available to be overwritten.

So as we overwrite our discs, they get overwritten. We're not retaining a record. We're not retaining a copy.

Mr. Blaine Calkins: It would only be there for a little while, until —

Mr. Colin McKay: It's the technical limit to how we do that.

[*Translation*]

The Chair: Unfortunately, Mr. Calkins, you're out of time.

[*English*]

Mr. Blaine Calkins: Oh, really? I was having so much fun here.

Thank you, Mr. McKay.

[*Translation*]

The Chair: Perhaps we can come back to you later.

Mr. Andrews, you have seven minutes. Go ahead.

[*English*]

Mr. Scott Andrews (Avalon, Lib.): I'll try to carry on in the same line.

Early on, when you talked about a person removing their history, just so that we get an idea, how many data points would you have on an individual, just so that we can get our heads around exactly how much information Google would have on a user? How long does that history go back?

Mr. Colin McKay: I'm afraid I can't give a direct answer on the number of data points, in part because the information we collect through your web browsing isn't used to identify specific data points about you, as an individual. It's used to create generic profiles about our users that could be then used for providing services and providing advertising. So there may be *x* number of data points that simply result in a conclusion that you like American-made cars. There's no specific line that way.

In terms of how long we retain that sort of information, if we're dealing with the web search history, there's a tool called Ads Preferences Manager, on which you can go in and take a look at the buckets we've identified as applying to your particular interests, and then correct them or delete them. You can either make the point to us that, as the example was made, someone is a hunter—that you're either a very specific kind of hunter or that you're not at all.

For example, from some of my search habits, sometimes Google thinks that I'm a 35-year-old woman. I don't know quite how it arrives at that conclusion, but I have to go in and correct it. It's a click on an X, and then that data point is erased and it's reconstructed, hopefully appropriately.

● (1600)

Mr. Scott Andrews: Part of that "do not track", again...as Mr. Calkins just talked about, the devil is in the details, from the commissioner. What are the defaults? When you look at the defaults, would you be opposed to regulations on what those defaults may be?

Mr. Colin McKay: You pose an interesting question, because you started by noting that it's a process of transition and it's difficult to determine what the appropriate defaults would be. Then you closed by asking if we should regulate that.

That's what forms my answer, which is that we're still in the process of evolution where we're trying to identify the appropriate format and the appropriate time and the appropriate content to help users make decisions about their data. We feel we made a tremendous step forward this year with our changes in our privacy policy, because we took what was a very long and complex document and broke it down to several very simple elements for users to really understand how we're asking for information and what we're using it for. That's an example of trying to take what is one big long notice and giving it multi-layered notices.

It's difficult to try to set regulations in terms of what should be included in those sorts of notices and that sort of discussion with the user without a period of experimentation. In fact, setting regulations often just sets the status quo in stone, and certainly in this space we're seeing innovation every week with regard to how we evolve our relationship with our users to make sure they are informed and have that sort of level of personal control.

Mr. Scott Andrews: Also, you're not the only player. How would you put these broad brushes across many browsers, many companies, to say these are the specific defaults that you would use?

Do you collaborate within the industry, yourself with the other players in the industry, to say these are the privacy guidelines that we'd like to follow generally as a group? Would that be a worthwhile exercise? Do you do that among other companies, as we speak?

Mr. Colin McKay: Yes, we do. The major online players as well as the offline players all regularly speak about privacy and data protection issues, and then, more specifically, we get involved in exercises both in Washington and in Brussels in trying to identify what the future challenges will be in this space as well as identify what's the appropriate level of response, whether it's on a company level, industry-wide level, or self-enforcing guidelines.

As well, for Google in particular, since we're so security-focused, we have an extreme level of interest and involvement in the technical side of every aspect of security online, which often butts up if not overlaps with privacy concerns. So I would say the level of cooperation and collaboration is great among the companies.

Mr. Scott Andrews: You mentioned Google Dashboard. Is there a one-stop shop for all this in Google for opting in and opting out? Is everything clear and concise within Google, or do you have to do it across every individual product?

Mr. Colin McKay: That's Dashboard. Dashboard is your list of the services you belong to as well as the options available to you, whether or not you want to use them and whether you want to opt out of specific services.

Mr. Scott Andrews: Thank you.

[*Translation*]

The Chair: Thank you.

It is now over to Mr. Carmichael.

[*English*]

Mr. John Carmichael (Don Valley West, CPC): Thank you, Chair.

Thank you, Mr. McKay, for your testimony today.

I want to ask you about enforcement. I appreciate how you position your relationship with the Privacy Commissioner. You share new platforms, new concepts, and new ideas as you bring these to market. I think I'm accurate, right?

Mr. Colin McKay: Yes.

Mr. John Carmichael: You basically take the package and look for feedback on where she may have some concerns, etc.

Do you believe that in Canada there is a need for stronger enforcement powers to cause companies to respect the privacy legislation in this country? Having your background in privacy, you're probably pretty well qualified to give us an honest opinion on that.

● (1605)

Mr. Colin McKay: Thank you for your question.

In my experience, we've seen companies react quickly and strongly to the Privacy Commissioner's rulings. In my personal experience, I've had some very constructive conversations with both the federal commissioner and the provincial commissioners about the products and services we're about to introduce or have introduced. There's a very effective dialogue that happens that encourages us to be innovative in the products and services we provide to Canadians while reinforcing that there is legislation in place that we must meet. We see that sort of dialogue as a very constructive way to continue to offer exciting and innovative products to Canadians.

A move to a system that is more enforcement-based would prompt some caution on the part of companies. In a system that was more heavily focused on enforcement, we would have to consider the possible repercussions of having that open a discussion of how our products roll out and how the Privacy Commissioner interprets our actions.

Mr. John Carmichael: Thank you.

For Google Takeout, it's my understanding that if I decide I want to leave, I take advantage of Google Takeout and I take everything with me.

Mr. Colin McKay: Yes.

Mr. John Carmichael: All my information, anything I have deposited within the Google framework, I pull out and I go away completely.

Mr. Colin McKay: Yes.

Mr. John Carmichael: Okay.

The question I have was more related to Canadians on Google. Do they have a privacy risk? Is there any risk at all, for a Canadian using Google, of having that privacy breached today?

Mr. Colin McKay: My response to you would be that we provide the most secure systems and services available to Canadians. We spend every day all day making sure that we not only identify but avoid the sorts of traps that lead to the inappropriate or illegal disclosure of information, whether it's personal or not.

Mr. John Carmichael: I hear you on that. There's a little motherhood and apple pie there, and I appreciate that.

When we started this study, one of the concerns we had was the privacy of the average Canadian. We know that in some arenas, there are all kinds of private information. My colleague on the other side referred to seeing a discussion that he didn't feel, maybe, he should be a part of, the way the conversations opened up within the architecture.

The concern we've had with respect to privacy in Canada is that we have to be absolutely certain that we're doing our job to ensure Canadians' peace of mind. We know that people give their information freely. There has to be a better education process, I think. At the end of the day, I'm very concerned that we have a privacy problem.

How much time is left, Mr. Chair? Do I have lots?

[*Translation*]

The Chair: You have three minutes left.

[*English*]

Mr. John Carmichael: Thank you.

What would you advise Canadians, as Internet users, do to protect themselves in a more stringent way when using the Internet? I'm thinking about all the different platforms out there and your background in privacy. How do we advise? What would you advise us to say to Canadians when we put our final report together? How do they protect themselves? How do we protect them? What do they need to do when they're on the Internet to ensure that their privacy is secure?

Mr. Colin McKay: Thank you for your question. I think you brought up a valuable point in mentioning the other member's conversation online, in that we're looking at a combination of measures in order to ensure continuing privacy online.

In addition to using secure services and ensuring that you're making the right decisions when using those tools, we also need to take the steps to make sure, as we evolve into a society that communicates online, that not only young people, but every generation has access to educational tools that allow them to work through how they should be sharing on social media sites, how they should be using online services, and the context within which they want to share information or make information public or restricted.

From our point of view at Google, we've undertaken things like an advertising campaign called Good to Know, which tries to walk users through the various examples of how their information is stored and shared online. We also partner with child safety and public education organizations like MediaSmarts right here in Ottawa and the Canadian Centre for Child Protection in Winnipeg to work on public education campaigns that go in to the classroom and give students that one-on-one advice on how to make the transition as a young adult into the online world. Then we more explicitly create things like the curriculum for teachers, and the citizens' curriculum around YouTube that helps individuals and students think about how YouTube fits in with the context of their being active and vibrant citizens.

To me there's a multi-phase process and a multi-step process that needs to take place. You're right; a lot of it is public education, and quite a bit of it is also providing the appropriate tools to users so that they have the choice of control.

● (1610)

Mr. John Carmichael: Just in closing—I think I'm probably down to the wire here—if I summed up, and correct me if I'm wrong, on Google my privacy is absolutely secure.

Mr. Colin McKay: Yes.

Mr. John Carmichael: It cannot be hacked.

Mr. Colin McKay: Yes: it cannot be hacked.

Mr. John Carmichael: So a privacy breach is a non-issue with Google.

Two, on Google Takeout I can pack my bag and leave with all my laundry at any time.

Mr. Colin McKay: Yes.

Mr. John Carmichael: Terrific.

Thank you.

[*Translation*]

The Chair: Thank you, Mr. Carmichael.

It is now Ms. Borg's turn for five minutes.

Ms. Charmaine Borg (Terrebonne—Blainville, NDP): Thank you, Mr. Chair.

I want to thank you, Mr. McKay, for joining us today.

Given your position as an industry leader in the digital market, your remarks are especially pertinent. I would say that everyone in this room is aware of all the technological innovation and new potential you are responsible for.

The purpose of our study is to ensure that users can access those tools with the assurance that their personal information is being protected. Given that yours is an international company, the question as to which policy you will adopt often comes up. Of course, we have laws and regulations here in Canada, but so do other countries.

My question is when you develop these policies, are they country-specific, or do you follow a model, for instance a European model.

[*English*]

Mr. Colin McKay: We have a company-specific model. Let me just ask if you're asking about specific requests for user information, or if you're talking about privacy law.

[*Translation*]

Ms. Charmaine Borg: I am speaking about policies on personal information.

[*English*]

Mr. Colin McKay: We have a company-wide policy that strives to meet all the obligations across all the countries.

[*Translation*]

Ms. Charmaine Borg: Very well. Thank you.

The term “personal information” is defined in a variety of ways. I would like to know which definition Google uses.

[*English*]

Mr. Colin McKay: We use the definition of our primary regulator, which is the FTC.

[*Translation*]

Ms. Charmaine Borg: Fine. Thank you.

So you can now make changes to information—and I think that's an excellent tool—if, for instance, you want to correct your age, as in the example you mentioned.

But if a Google user doesn't change the default settings, will that person's information end up being destroyed or kept forever? I am referring to search engine optimization data or previously visited sites and so forth.

[*English*]

Mr. Colin McKay: It could be destroyed forever. If, in the case of websites, you've allowed us to record your web search history, and then you decide to turn that off, then that's gone.

[*Translation*]

Ms. Charmaine Borg: Let's assume I'm a first-time Google user, and I don't change the default settings. Will that information be destroyed at some point if I don't change or delete it on my own initiative?

[*English*]

Mr. Colin McKay: It's a difficult question to answer because it's an evolutionary process. As you're using the web search, we're not trying to serve results to you that deal with your needs in the past. We're trying to serve results to you that deal with what you're looking for right now. However, we can get insight over time into what you're interested in, what you're looking for, and which results you did not find useful.

There are elements of all of that data that don't necessarily pertain to you as an individual, but that we find useful in developing new products and new tools. The distinction you made originally between personal information and other data that could be associated with your activities, but isn't associated with you, is a useful one for us.

I would say that at some point we do not retain all the data that we collect, simply because it's not useful to us. At the point where it no longer becomes useful, we delete it. We're not in the business of creating a very large bucket of information about you. We're in the business of providing very useful services and products to you as an individual.

● (1615)

[*Translation*]

Ms. Charmaine Borg: Clearly, that data is less pertinent 10 years later. Is there some kind of mechanism in place that destroys that data? Is it done systematically?

[*English*]

Mr. Colin McKay: Yes, there is. It's just.... It's not one simple answer. The reason I'm pausing is simply because, depending on how valuable that log information is—for example, in fighting malware—we may keep it for *x* period of time. For web search history, it may be a different period of time. But it's certainly not a case of 10 years, and it's not a case of multiple years.

[*Translation*]

Ms. Charmaine Borg: Thank you.

My next question is on a different topic.

Companies and social media sites commonly change their terms of use and privacy policies quickly, in order to adapt to the equally fast-changing technological landscape.

In that environment, how can we be certain that user consent is ongoing and informed?

[*English*]

Mr. Colin McKay: Thank you for that question.

You're right: there's a constant evolution. When we look at the marketplace right now, not just at our product but at any company's products, you can see this in your daily experience. The screens and the notices that you're given when you sign up to use new products, to download apps, and to use new hand-held devices are constantly changing, because they're reacting to consumer needs. They're reacting to the input of privacy and technological advisers.

We're arriving at a place where we're starting to see notices that are more complex—sorry, not more complex, but that give you more information about the decisions you're making at that moment and that give you the opportunity to make an immediate decision about whether this service is actually useful to you. In fact, what we're seeing in one of our products on the android phone is that people are making decisions not to download an app, based on the information that's provided to them in the sign-on process. The sign-on process has gotten to a point where it's clear enough, in that they've arrived at a piece of information and have said that the usefulness of the app is not valuable enough for them to make that trade-off.

[*Translation*]

The Chair: Unfortunately, your time is up, Ms. Borg.

It is now Mr. Butt's turn for five minutes.

Mr. Brad Butt (Mississauga—Streetsville, CPC): Thank you, Mr. Chair.

[*English*]

Thank you very much, Mr. McKay, for being here today. Again, on behalf of the committee members who did go to Washington, thank you again for the opportunity to visit your location in Washington and, certainly, to learn more about what the organization is doing.

When we visited and learned about what the challenges are around privacy in the U.S. as well, I think what we took back is that there isn't as robust a regime in the United States currently as there is in Canada, even though part of what we're doing here as a committee is reviewing our privacy protection, .obviously, and making sure that we're up to date with how fast the world is evolving over the Internet and through social media.

I know that at Google Canada in particular you've had I believe a fairly positive working relationship with our Privacy Commissioner. I know that we've been wrestling with her role and the role of her office in overseeing these issues and obviously in dealing with complaints if they emanate through to her office, and also with what roles and responsibilities, beyond what she currently has, that we should be looking at.

I think it's helpful to get advice from the organizations with which her office is interacting. Obviously, financial penalties have been raised, and also some other increase in her adjudication role. There have been different schools of thought on that, as to whether that is better, worse, or fairer. Some people have said that it would make her the judge, the jury, and the sentencer all in one. Others have said that maybe the Privacy Commissioner does need those additional roles.

Have you folks looked at that in any more significant way? Have you compared and contrasted the regulations by the Federal Trade Commission in the United States—under which you're operating, to some degree—versus being under the auspices of our Privacy Commissioner here? Are there any specific things that you folks have learned from it that might be helpful to our committee in looking at some recommendations?

● (1620)

Mr. Colin McKay: I'll leave my comments to the Canadian situation. As you know, I have plenty of American colleagues who deal with the FTC and the other agencies on a daily basis.

In Canada we have the advantage that we have a national private sector privacy legislation, and we actually have national private sector privacy legislation that is comparable to, and is in fact complementary to, legislation in some particular provinces. What that has meant operationally for our company is that we have a consistent set of standards across the country, across all our product lines, that we know we have to meet. And we meet them on a daily basis.

We also know that we have a relationship with the privacy commissioner at the federal level and the provincial levels where we can speak to them if we have questions about the application of that legislation, and we can speak to them about what may be developing in terms of technology, even long before there's an actual product, so we can arrive at an understanding of what compromises and what sort of tools have to be made available to users in order to reflect the privacy legislation in Canada and the needs for data protection and security of the users. We've seen that this works.

You mentioned financial penalties. In my experience, we've seen companies, particularly in the online space, be the subject of investigations and reports by the Privacy Commissioner and then react very strongly and very quickly to resolve the concerns of the commissioner as identified.

There are many more cases where there are complaints and those issues are resolved in dialogue with the commissioner's office. The difficulty we would face moving to a regime such as is available in some countries in Europe is that the relationship becomes more cautious. If you are dealing with a data protection authority that has the ability to levy financial fines, there's a caution in how you engage in dialogue with that authority, both in terms of making sure that you've set limits very clearly and that you're very aware of the implications of that engagement.

I would say that we really have an advantage here in Canada, certainly compared with the United States, in having that consistent legislation across the country. We've seen 10 years of it being applied fairly well, with very few instances where companies have not responded to the reports delivered by the commissioner.

Mr. Brad Butt: I have a daughter who is turning 13 on Thursday, and she is very social media-savvy. She doesn't get it from me; she must get it from her mother. I'm always concerned about children and their use of social media.

I don't want to stifle their ability to participate and be creative and interact with their friends and all that. I think it's good. I mean, that certainly wasn't around when I was 13, right? I think it's wonderful that they can do that. They can share things and get access to information worldwide, instantaneously. It's neat stuff. But as a parent, I still question how to make sure her privacy, her personal life, isn't somehow invaded.

Do you see, as an organization...? In answering some of Mr. Carmichael's questions, I think you provided some very good evidence to show how strong a privacy policy you have, that people can take their stuff and run, if they feel there is an issue, they can go and it's done and their privacy has been protected.

But do you see a different role for underage users versus adult users? Have you developed anything to monitor that within the organizations, that we're making sure that, you know, the Sarah Butts of the world are protected versus the Brad Butts of the world—who's probably old enough to know better?

[*Translation*]

The Chair: I'm going to have to ask you to wrap it up in 30 seconds.

[*English*]

Mr. Brad Butt: And I said “probably”. I didn't say “for sure”.

Mr. Colin McKay: To be brief, as the chair has asked, I have three children over the age of 12, and in many ways it's the same debate we've had as parents for eternity: how do you learn to control people who are becoming young adults, whether it's online or offline?

But you're right, there's a clear need to provide tools both for young people as well as their parents, to understand the tools they are using, the environment in which they are using, and the benefits and the costs of how to use them.

I mentioned in my notes that Google+ was built specifically with this conundrum in mind, trying to provide a tool for young adults that allows them to communicate but within an environment that reflects that they may not necessarily fully understand the impact of what they're about to do, and also trying to isolate them a bit from those larger societal impacts of their engagement online.

Mr. Brad Butt: Thank you very much, Mr. Chair.

● (1625)

[*Translation*]

The Chair: It is now over to Mr. Boulerice.

Mr. Alexandre Boulerice (Rosemont—La Petite-Patrie, NDP): Thank you, Mr. Chair.

Thank you very much, Mr. McKay, for being here today. We quite appreciate it. You were obviously indispensable to our study.

From what I gather, when we surf using Google, you keep data on the footprints we leave all over the Web, information on what our interests are, which sites we visit and so on. You then use that information to seek out advertisers looking for specific profiles. That's the word you used earlier. You build profiles. Is that right?

[*English*]

Mr. Colin McKay: Yes. I wouldn't specifically say “profiles”, because that implies a level of personal engagement that doesn't exist. It's more buckets of information about demographic groups and specific interests rather than actual profiles.

[*Translation*]

Mr. Alexandre Boulerice: Earlier, Charmaine and I were talking about skiing. If I'm someone who reads ski magazines or goes on skiing sites or sites that sell sports equipment, it is highly likely that the name of an advertiser who sells skis will pop up. You also said that there is now an “incognito” option.

Mr. Colin McKay: Yes.

Mr. Alexandre Boulerice: So all of my interests and surfing activity are rendered invisible or non-existent on your end.

[*English*]

Mr. Colin McKay: Yes.

[*Translation*]

Mr. Alexandre Boulerice: What percentage of Google users browse in “incognito” mode?

[*English*]

Mr. Colin McKay: I don't have that in front of me right now. It's not insignificant. Also, the way people use it, they use it selectively. They may have specific searches that they don't want any record being held, or they may simply, as I explained, be using a device they do not have usual control over. They choose to use that tool, so there's no trace left of their usage on the machine itself.

[*Translation*]

Mr. Alexandre Boulerice: So if everyone used that mode at all times, you would lose a tremendous amount of money.

[*English*]

Mr. Colin McKay: No, you know how I would phrase that? I would actually turn it around. I would say that if everyone used that mode, and you had advertising that was less relevant to your specific interests as a skier, or as a hunter, or as a parent, you would have more generic advertising that would be less effective.

This would mean that businesses would have to spend more money, advertising with very broad and clumsy tools, to try to attract their customers, so in fact we would all find that more expensive.

[*Translation*]

Mr. Alexandre Boulerice: That's an interesting answer.

I want to pick up on something my colleague, Ms. Borg, mentioned. It had to do with the idea that, under the terms of use, one can select an option that enables you to override Canadian laws in favour of foreign ones. That option exists currently. Don't you think Canadian laws should take precedence over foreign laws here in Canada, from Google Canada's standpoint?

[*English*]

Mr. Colin McKay: Are you speaking specifically about privacy legislation?

[*Translation*]

Mr. Alexandre Boulerice: Yes.

[*English*]

Mr. Colin McKay: In effect, Canadian privacy legislation, since it has a comprehensive national impact, is in some ways stronger than that in the United States. We feel we meet Canadian privacy legislation, just as we meet European privacy legislation. In effect, by meeting Canadian and European privacy legislation, that boat is floating to a higher level. We're meeting that higher standard.

[*Translation*]

Mr. Alexandre Boulerice: Every company and every government has its own rules and legislation. On top of that, users have to deal with the reality of all the different definitions of what constitutes personal information, either for the multitude of tools or for the social media out there. At some point, users don't really know what definition Facebook or Google uses, or which laws apply where they live.

Don't you think that could lead to a sort of mass confusion?

[*English*]

Mr. Colin McKay: We're very specific about the information we collect and why we're collecting it from users. We're also very specific about the information we don't use in creating these buckets and providing services to advertisers. Some of the information that you would consider the most sensitive, whether it's political views or whether it's health issues, we don't consider at all. Then in other instances, when you're using our products, like Google+, it's very explicit to you why you're providing this information and why we're using it.

That's the farthest we can go; we can be honest with you, as a user, on why we need this information and how we're going to provide the service to you that would require this information.

● (1630)

[*Translation*]

Mr. Alexandre Boulerice: Thank you. I think my time has run out.

The Chair: You are absolutely right, Mr. Boulerice.

There's no else on the list, so I'm going to take the opportunity to ask you a question of my own. That's something I seldom do.

I have to tell you, I wasn't aware of “incognito” mode before. My question has to do with the potential of people using it for nefarious or illegal purposes, such as child pornography. Can you still retrieve some data, or is it impossible, even in specific instances where the option could benefit certain individuals?

[*English*]

Mr. Colin McKay: In the situation you're describing, there's a level of complexity. When we're talking about the incognito mode, we are not collecting information about your searches. We're not collecting information about your behaviour in using the browser.

If you're, in fact, talking about behaviour that could be damaging or illegal or seditious, you're likely engaging in other activities that would then signal or send a flag, or be noticeable through other forms of communication and transmission online. Those would be more traditional log analyses, the sort of materials we use and every company and every government uses to identify illegal behaviour. But incognito mode itself, you're right, is a very secure tool that offers a confidence to the user.

[*Translation*]

The Chair: Thank you.

Thank you for appearing before the committee today. It was a real pleasure to have you.

For the committee members, I want to clarify that our meeting will now continue in camera, since we will be discussing witnesses and the list is not yet public information.

Once again, thank you to our Google representative, Mr. McKay, for speaking to us today.

[*Proceedings continue in camera*]

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

SPEAKER'S PERMISSION

Additional copies may be obtained from: Publishing and Depository Services
Public Works and Government Services Canada
Ottawa, Ontario K1A 0S5
Telephone: 613-941-5995 or 1-800-635-7943
Fax: 613-954-5779 or 1-800-565-7757
publications@tpsgc-pwgsc.gc.ca
http://publications.gc.ca

Also available on the Parliament of Canada Web Site at the following address: http://www.parl.gc.ca

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

PERMISSION DU PRÉSIDENT

On peut obtenir des copies supplémentaires en écrivant à : Les Éditions et Services de dépôt
Travaux publics et Services gouvernementaux Canada
Ottawa (Ontario) K1A 0S5
Téléphone : 613-941-5995 ou 1-800-635-7943
Télécopieur : 613-954-5779 ou 1-800-565-7757
publications@tpsgc-pwgsc.gc.ca
http://publications.gc.ca

Aussi disponible sur le site Web du Parlement du Canada à l'adresse suivante : http://www.parl.gc.ca