House of Commons
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 030 • 3rd SESSION • 40th PARLIAMENT

EVIDENCE

Thursday, November 4, 2010

Chair

The Honourable Shawn Murphy

Standing Committee on Access to Information, Privacy and Ethics

Thursday, November 4, 2010

● (1530)

[*English*]

The Chair (Hon. Shawn Murphy (Charlottetown, Lib.)): I will now call the meeting to order. I want to welcome everyone here today.

This meeting, called pursuant to Standing Order 108, is to continue the committee's study on street imaging applications.

The committee is pleased to have before it this afternoon Mr. Jacob Glick. Mr. Glick is the Canadian policy analyst with Google Inc. Of course, we did have representatives from the Office of the Privacy Commissioner here last week to talk about this issue.

We only have Mr. Glick for approximately an hour, so I'm going to get going right away. I understand he has some opening remarks, so at this point in time I'm going to turn the floor over to you, Mr. Glick. Again, welcome to the committee.

Mr. Jacob Glick (Canada Policy Counsel, Google Inc.): Thank you very much, Mr. Chair, members of the committee.

Thank you very much for this opportunity to meet with you to discuss Street View and Google's mistaken collection of Wi-Fi payload data, and to answer your questions.

My name is Jacob Glick. I'm Google's Canada policy counsel. In this role, I work with regulators, policy makers, academics, civil society, and industry on public policy issues affecting Google and the open Internet. In Canada, Google has offices in Waterloo, Toronto, Montreal, and Ottawa. Google is consistently named one of the best places to work in Canada. Our Waterloo and Montreal engineering offices are developing products that are used by hundreds of millions of people globally, and these offices are expanding significantly.

To begin, I would like to update you on Google's Street View products, since Mr. Lister appeared before this committee in June 2009. We have had a very successful rollout of Google Street View in a way that showcases how privacy and innovation can be combined to produce successful leading-edge services for consumers.

Prior to launching Street View in Canada, we addressed all of the concerns identified by this committee and by the Privacy Commissioner. We've implemented the most sophisticated blurring technology to blur faces and licence plates in all of our images. We've implemented a quick and easy takedown procedure. Anybody can request that Google remove pictures of themselves, their house, their kids, or their car, from Google Street View. Finally, we are permanently baking in this blurring after one year.

Canadians are avid users of Street View. In fact, in absolute numbers, Canadians are the third most active users of Street View in the world, behind only the U.S. and the U.K. Since its launch, Canadians from coast to coast to coast have used this next-generation cartography to map their way to the store, promote their local business, sell their house, and explore our country online.

In addition to updating this committee on the successful rollout of Street View, we want to talk to you in particular about the Wi-Fi matter, which is not, strictly speaking, part of Street View, but which used Street View vehicles as a platform.

Let me start by saying we are very sorry this happened. What happened is not consistent with our commitment to serving Internet users, and frankly, we are embarrassed about this.

I want to give you an overview of what happened, how we found out, what we did immediately, and what we are doing to prevent it from happening. After that I'll be happy to answer your questions.

To begin, I want to underscore some important facts for this committee. No payload data transferred over encrypted networks were collected by Google. Google had no desire to use payload data in any way. No payload data have been used in any Google product or service, and none of the Canadian payload data have been given or disclosed to third parties; it has been segregated and secured.

So what did happen? As you know, in 2007 Google was preparing to launch Street View and was deploying a fleet of vehicles around the world to collect street-level imaging. At the same time, an engineer with our location-based services group had the idea of using Street View vehicles as a platform to do what many other companies have done, which is detect Wi-Fi hot spots to support location-based services.

Using publicly broadcast Wi-Fi hot spots as landmarks to help users identify where they are is common industry practice. The engineer designed software code to collect Wi-Fi network data, and unfortunately, also Wi-Fi payload data. Payload data refers to the contents of transmissions.

Google did not want this payload data and does not believe that collecting such payload data is useful or appropriate.

The engineer should have flagged, for Google's in-house lawyers, the plan to collect Wi-Fi payload data. He did not do so. If he had, this would have been an opportunity at the outset of the program for Google to identify the problem and stop it. As a result, the code was deployed on Street View vehicles. The software worked as it was programmed to do, collecting Wi-Fi network data and Wi-Fi payload data sent over unencrypted networks.

In April of this year Google was asked by the Hamburg Data Protection Authority to audit the Wi-Fi data collected via Street View vehicles. We carried out that audit and discovered that Wi-Fi payload data were being collected in addition to the network data. Before announcing publicly what we discovered, I personally called Commissioner Stoddart and advised her of this issue.

After that, Google made a public announcement and apologized for what had happened. To be clear, Google did not want this payload data. Its collection was a mistake. Shortly after I advised Commissioner Stoddart that payload data had been collected in Canada, she began an investigation into this matter. We cooperated with her and provided her investigators with access to the Canadian payload data at our corporate headquarters.

To provide some context into the comprehensiveness of this investigation, the Privacy Commissioner's investigators were the only data protection authorities globally to conduct their review into this matter at Google's headquarters in California. The commissioner has issued a preliminary letter of findings; we accept her findings. We are committed to resolving this matter.

We have been asked, how could this data be collected without Google knowing about it? First, to provide some context, the Wi-Fi payload data represents a small amount of data, relatively. All the payload data collected in Canada could fit on a standard-sized USB thumb drive that you could buy at Best Buy or Costco. Also, the data was written onto the hard drives in the cars in a raw form, meaning it cannot be understood or recognized unless processed to be human-readable. Other than the engineer who wrote the code, no one at Google had any plans to use this data, so there was no trigger for anyone to look at it.

It's important to note that Google had no desire to collect the payload data or to use the payload data in any way. To be clear, Google has not used this data in any product or service. Regardless, there is no excuse for Google having collected this data. As soon as Google discovered that they had been mistakenly collecting Wi-Fi payload data from unencrypted Wi-Fi networks, all of the Street View vehicles around the world were grounded. All of the Wi-Fi payload data was immediately segregated and secured. Note: nobody has reviewed the Canadian payload data, other than the Privacy Commissioner's investigators and those who facilitated their investigation. It has not been disclosed to any third parties.

It's fair to ask, what measures is Google putting in place to ensure this never happens again? First, Google began a comprehensive investigation to determine how this happened and what steps need to be implemented to make sure this never happens again. Google commissioned an independent third party to review the code. That independent report has been made public on our blog, and it was provided to the Privacy Commissioner during her investigation.

Further, I can report that on October 22 Google announced a number of significant changes to its privacy practices and controls. Prior to announcing these publicly, I personally spoke to Commissioner Stoddart to advise her of these changes. She also discussed them in more depth with my colleagues last week. Specifically, these announced changes were as follows. First, Google appointed Dr. Alma Whitten as our director of privacy to ensure that we build effective privacy controls into our products and internal practices. Dr. Whitten is an internationally recognized expert in the computer science fields of privacy and security. Second, we are enhancing our core privacy training with a particular focus on the responsible collection, handling, and use of data. Finally, Google is adding new safeguards to our existing privacy compliance system to include independent internal audits to ensure that user privacy is protected.

We are of the view that these changes will significantly improve our processes and controls to prevent something like this from happening again. That is where we are now. We're sorry this happened. We've learned from it, and we are improving our processes as a result.

I would be pleased to answer your questions.

Thank you, Mr. Chair.

● (1535)

The Chair: Thank you very much, Mr. Glick.

Now we'll proceed to the first round of questioning, and that is going to be for seven minutes each. We're going to start with you, Mr. Easter.

Hon. Wayne Easter (Malpeque, Lib.): Thank you, Mr. Chair.

Welcome, Mr. Glick, and thank you for your presentation.

I don't mind admitting I have a bit of difficulty getting my head around some of this modern technology stuff. Can you explain to me, in layman's terms really, what payload data is, and basically how the system acquires what you call “payload data”?

● (1540)

Mr. Jacob Glick: Sure. Thank you very much for that question. It's an important technical question. I should apologize before starting to answer it to say that by training I'm a political scientist and a lawyer. I happen to be a big nerd, so I think I will be able to answer your question as best I can. But if there are follow-up questions about where I am unclear, I'm happy to offer any clarifications.

The Chair: You can always Google it.

Hon. Wayne Easter: I could have Googled it, I suppose.

Mr. Jacob Glick: Right. I use all the search engines, so you could Bing it, you could do Ask.com.

Hon. Carolyn Bennett (St. Paul's, Lib.): Do you want me to Google it for you?

Mr. Jacob Glick: Your colleague is going to Google it for you on her BlackBerry. But in the meantime, my understanding is as follows.

When transmissions are sent over the Internet, those transmissions have two components: headers and payloads. The "header" is basic identifying information, and in this case it was the identifying information of the network itself that we were attempting to collect. That is, for example, if you're in Starbucks there's the name of the router. The better example is you open up your laptop and you say, which Wi-Fi networks are around me—because all of your laptops have Wi-Fi built into them—and it says there are these five Wi-Fi networks. That's the information we were looking to collect, the name of the network and some associated technical information that relates to the network. That's the same information you see on your BlackBerry when you turn it on, and it looks for available Wi-Fi networks.

The other component is the actual data that get transmitted over that network. So, for example, if I'm surfing the Internet and I'm looking at vacation homes in Florida, the contents of the web pages that are transmitted are the payload data.

So that's the difference between "network data" and "payload data". "Network data" is the name of the wireless hotspot, and "payload data" is the actual content of the transmissions sent over the network.

Did I answer your question?

Hon. Wayne Easter: Somewhat. I may have to Google it to—

Hon. Carolyn Bennett: No, here it is.

Mr. Jacob Glick: I should add to all of this that we've had a number of blog posts on this topic as well.

Hon. Carolyn Bennett: The third on the Google search is your apology.

Mr. Jacob Glick: Excellent.

Hon. Carolyn Bennett: "Failed badly", it says.

Mr. Jacob Glick: Right. I think that's consistent with my testimony.

Hon. Wayne Easter: Last night I did, with another individual, look at the Street View, and there's no question you can zero right in on a place, although it's back a period of time and there is the blurring of the individual's identity, basically. But I guess if you knew the person, you could still identify them.

One of the original concerns that I think was laid out by this committee and the Privacy Commissioner was not having individuals' prior knowledge or consent. Google is claiming now that you have all those concerns covered. How so?

Mr. Jacob Glick: We worked with the Privacy Commissioner on this very issue, and they were satisfied that posting information about where and when we would be driving, and making that available publicly and to the media, was a sufficient notification that would satisfy them that our obligations under privacy law would be met. I should say that when you think about the extent of publicity that the collection of the Street View data got, I think that's borne out. What I say sometimes when I talk to people about this is, this is the best-publicized cartographic collection in the history of the country. The fact of the matter is there are competitors of ours who have similar-type services, street-level imaging services of communities in Canada, and you might not know about those ones, even though they've undertaken similar types of notices with the media under the direction of the Privacy Commissioner.

Because Google is a big company, we get lots of media attention, but the fact is that the collection of this Street View data in particular got incredible amounts of media attention, and at the end of the day the commissioner, as I understood it, was satisfied with that.

● (1545)

Hon. Wayne Easter: I didn't know you were in my own area, but I was told a Google car went down the road doing its photography.

How do you prevent a lot of property information from becoming available, information that some property owners might not want available? How do you prevent that?

Mr. Jacob Glick: We have a robust takedown procedure, which allows anybody to report a problem on any image they see. And if they see themselves, their houses, their kids, or their cars, they can request that Google take it down. We process those requests in English and French, typically within 24 hours. So if you see your property there, and you say you don't want your house on Street View or—

Hon. Wayne Easter: Sorry, I don't want to interrupt, but not everybody is going to see this. Not everybody knows it's out there. In this system of cyberspace, if I were to send an e-mail criticizing Pierre Poilievre, it'd be in super cyberspace forever. And he'd be offended. He'd never forgive me.

Mr. Pierre Poilievre (Nepean—Carleton, CPC): He'd never do that to me.

Hon. Wayne Easter: My concern is this. Yes, it's taken down, but you have a lot of people who might be offended and not know it's there. Once it's there somewhere, isn't it always there? That's what I find about this system.

The Chair: Go ahead, sir.

Mr. Jacob Glick: The short answer is, once we take it down, it's down.

But the longer answer to your question is.... What do people do when they don't have access to computers and therefore don't have the opportunity to take it down? Statistics show that sizeable numbers of Canadians are using this on a daily basis, not every Canadian obviously, but it's a very popular product, as I indicated in my opening statement. More Canadians use Street View than Japanese people, not per capita but in absolute numbers. It's an incredibly popular and useful product. Many of us who can't read maps can understand basic cartographic information. So it is a useful service in that regard. But obviously we're trying to balance the usefulness of it with the important privacy considerations that this committee, the Privacy Commissioner, and others have raised. And we think we've done that.

The Chair: Thank you very much, Mr. Easter.

We're now going to go to Monsieur Nadeau.

[*Translation*]

Mr. Nadeau, you have seven minutes.

Mr. Richard Nadeau (Gatineau, BQ): Thank you, Mr. Chair.

Welcome, Mr. Glick.

In view of the privacy commissioner's recommendation, I would like to know who is in charge of confidentiality for Google.

[*English*]

Mr. Jacob Glick: I apologize in advance. I don't speak French. The translation said in charge of confidentiality, but I presume you mean in charge of privacy.

The Chair: Monsieur Nadeau, do you want to repeat—

[*Translation*]

Mr. Richard Nadeau: In view of the privacy commissioner's recommendation, I would like to know who is now in charge of confidentiality for Google. Is there an individual, an employee or a vice-president who would be in charge of confidentiality?

[*English*]

Mr. Jacob Glick: The short answer is that Dr. Whitten has taken responsibility to be our director of privacy. That means not only is she going to be in charge of leading engineering teams working on privacy issues, as she has done already at Google, but she also will have heightened responsibility within Google to coordinate engineering teams and product teams at the highest levels of management. She reports now to the head of engineering and the head of our product division.

At a company such as Google, which is so innovation-driven, so engineering-driven, it's important to have somebody with a computer science background, somebody who has a doctorate in computer science, who can really speak the language of the product teams to really effect change. So part of that top-down change and part of that responsibility will be Dr. Whitten. Of course, we also have embedded people throughout the organization who have various kinds of accountabilities for privacy.

I can go into much more detail about this if you're interested.

● (1550)

[*Translation*]

Mr. Richard Nadeau: Yes, I will be interested.

You can give answers about this after other questions. You mentioned Dr. Whitten's main responsibilities.

What is Dr. Whitten's background? Has she been working in a similar company before or is she coming directly from the university? What is her training before she worked on this extremely important issue?

[*English*]

Mr. Jacob Glick: She's been at Google for a number of years. I don't have her biography in front of me, but we can use Microsoft Bing later to search for it and get it. But I can tell you that her doctorate is in the area of computer science and security and that she has published numerous papers in computer science, security, and privacy. She has been a thought leader in the area of privacy and security on a global basis for a number of years, and within Google. She has a deep understanding of these issues.

Another important thing to note, and I think this is an interesting bit of colour, is that she's based in London, England. She's not based in Mountain View, California. That's important because she doesn't bring a uniquely American perspective to bear on this; she brings a global perspective to bear. So to the extent that you think there are only American conceptions, for example, of privacy, I would respond that we're really talking about bringing global perspectives to bear in the design and implementation of privacy principles, practices, and standards that are already in Google, that have already contributed to the development of products that we have. She's been a leader in a number of initiatives already within Google, and that perspective will continue to be brought to bear at the highest levels.

[*Translation*]

Mr. Richard Nadeau: I would like to ask another question on a different subject.

Unless I misread something, Italy set rules before Google began street level imaging. For example, if I am not mistaken, it should be announced on your website at least three days ahead of time that you will be at such a place in Italy to make photos. This should also be advertised in two local newspapers.

Is that the way things are done in Italy?

[*English*]

Mr. Jacob Glick: I'm not familiar enough with the particular rules around collection in Italy. I can tell you that on the question of notice and collection in Canada, I personally was—

[*Translation*]

Mr. Richard Nadeau: I read that in the documentation we were handed. A radio station should also announce that Google will be in the area for its imaging operations. Another requirement is that cars should be clearly identified, and that stickers indicate that photos will be taken.

You said you are not familiar with this, but would you agree that this rule apply throughout Canada also?

[*English*]

Mr. Jacob Glick: We worked with the Privacy Commissioner to develop something that made sense under Canadian law and that she was comfortable with, and that we thought this committee and Canadians would be comfortable with, for notifying Canadians prior to collecting the data. As you rightly pointed out, all of our cars are clearly marked—and this is on a global basis—and they are visibly Google cars, and we have a website that we constantly update with information about where we're going to be collecting information.

In terms of the precise day and time and the precise neighbourhood, there is a level of complexity here that we have to acknowledge. These are moving vehicles that depend on certain weather conditions and certain other externalities, and it's hard to predict with precision where and when they will be. But, in general, we provide what we think is full and appropriate notice, both here in Canada and around the world, albeit the precise content of that notice may vary slightly.

But there's another important point I would like to emphasize on this issue in particular. Google is not the only company that is collecting street-level imaging in Canada. In order to create the GPS maps that are used in most of your cars and on websites where you access digital maps, the companies that create those maps, the companies that collect the digital information, follow a very similar process and take photographs of every street and every house. And they don't provide any notification, that I'm aware of, to anybody. They haven't received any scrutiny from a regulatory perspective on this, that I'm aware of, and they're not under the same obligations we are in terms of any kind of retention of that data.

So when comparing what our competitors are doing with what we're doing, it's important to put that into a broader perspective, that every digital map you use is created using a process of street-level photography. That's how maps are created today.

● (1555)

[*Translation*]

The Chair: Thank you, Mr. Nadeau.

[*English*]

Mr. Siksay, for seven minutes.

Mr. Bill Siksay (Burnaby—Douglas, NDP): Thank you, Chair.

Thank you for being here today, Mr. Glick. I agree that this is a very, very serious matter we've called you about.

I want to come back to the appointment of Dr. Whitten as Google's director of privacy. You said she's based in London and that she reports directly to the head of engineering and the head of production.

Where are those two folks based?

Mr. Jacob Glick: They're based in California.

Mr. Bill Siksay: Now, I know you're probably masters at communication across long distances, but London seems a bit removed from where the actual engineering and product development work are being engaged in.

How does Dr. Whitten engage with those folks who are doing that work?

Mr. Jacob Glick: There's a long answer. The short answer is that I think she's going to be a more frequent flyer than she is today. So if she's not super elite already, she will be.

But more to the point, Google has product development happening all over the world. Just 200 kilometres from here, in Montreal, we have some of the most talented engineers in the world working on products that aren't designed for Canada but for Google users globally. So it's not the case that all product and engineering decisions are happening in Mountain View, California; they're happening all over the world.

One of the interesting privacy-related products that Google released last year is the Google Dashboard, which—

Mr. Bill Siksay: Okay, that's great. We'll hear about products another time.

Mr. Jacob Glick: Sure.

Mr. Bill Siksay: I want to get to the whole issue of privacy and who looks after that.

So you say there are product development people here in Canada. Who is their supervisor? Who do they work with on privacy considerations relating to the products they're developing specifically in Canada?

Mr. Jacob Glick: The product teams in Canada will have responsibility, in the same way that product teams throughout the world will have responsibility, for privacy. That is say, every single engineer, herself or himself, is responsible and accountable for the collection, use, and handling of data, and we're going to be deepening that.

In addition, their managers are responsible for maintaining accurate product plans that accurately describe how products work.

In addition to that, they have lawyers assigned to every single product that Google has, who review product designs, plans, and implementation for legal compliance reasons, including privacy.

In addition to that, we do regular compliance audits of all of Google's products, and we actually just completed an audit of 200 products recently. So there are—

Mr. Bill Siksay: Was that system in place, though, when the Street View product was launched and the Wi-Fi hotspot component was missed? I gather that was developed in California. Is that system, with all of those people you've just mentioned, in place now, or is this a new system that's been put in place since the foul-up with that product?

Mr. Jacob Glick: What I described to you is a combination of both. So the answer is, we have always had privacy considerations be an important component of product design, and our products reflect them. This incident is an anomaly, but that's not to excuse it. I don't excuse it, and that's why we are building additional safeguards to try to make sure that something like this doesn't happen again.

● (1600)

Mr. Bill Siksay: Will there be a list of Canadian individuals who are designated to look at privacy issues for Google in Canada? That seems to be one of the recommendations of the Privacy Commissioner, that there be clearly designated and identified individuals actively involved in the process and accountable for compliance with Google's obligation under privacy laws. Is there now, or will there be, a list of folk who are responsible for that here in Canada for Google?

Mr. Jacob Glick: The way Google operates, because we don't operate on a traditional subsidiary model in which there is a president of Google Canada and a chief of finance at Google Canada, and all that, the answer to your question is that there are and there will be even more people who are responsible and accountable for privacy within Google, starting with Dr. Whitten, but not ending with Dr. Whitten. There will be people in Canada who are part of that team, but that will be a global team.

Mr. Bill Siksay: Okay. One of the other recommendations of the commissioner from the middle of October was that Google delete the Canadian payload data it collected. Has that been done, or what's the plan there?

Mr. Jacob Glick: My understanding of the commissioner's report is that she was asking us to delete the payload data after the resolution of the complaint. The finding that she issued was a preliminary letter of finding. In the way the administrative process works within her office, ultimately there is a final finding that comes out.

Presumably, that will come out in February, after we've responded to her, so I took her report to mean that we should be deleting the information after February. If I'm wrong about that, I'd be happy to go back to the commissioner and discuss this issue. We don't want to have this data.

Mr. Bill Siksay: It strikes me that the commissioner is saying it should be deleted immediately, unless there's some reason.... Has Google determined that there's some reason for not deleting it immediately? You're saying you're waiting until after February. That's months away—

Mr. Jacob Glick: The answer is, we haven't undertaken that analysis, but we will. If we're permitted to delete it, we'll delete it.

Mr. Bill Siksay: When is that analysis going to happen? We're a few weeks into having received this report. I suspect you had similar reports from other places, and you say you've secured the data, you've segregated it, so what's stopping you from deleting it right now? Why wait until February?

Mr. Jacob Glick: I promise, the moment I leave this committee, to make a phone call and ask that that analysis begin.

Mr. Bill Siksay: Okay.

Mr. Jacob Glick: I should add that in other countries around the world we have deleted the data at the request of the privacy commissioner in that jurisdiction where we've been permitted to by law, and in this case, when I called the Privacy Commissioner about this issue in May, I asked her specifically what she wanted done with the Canadian data, whether we ought to preserve it or delete it then. She advised me that we ought to delete it then, and that's what we did for Canada.

Mr. Bill Siksay: You deleted the data?

Mr. Jacob Glick: Sorry if I misspoke.

Mr. Bill Siksay: Yes. I'm confused.

Mr. Jacob Glick: She advised us at that time to preserve the data, and we preserved it.

Mr. Bill Siksay: All right.

You mentioned other countries where the data has already been deleted. Is that because that data was held in those countries and not transferred to a third country, as it has been in Canada's case?

Mr. Jacob Glick: No.

Mr. Bill Siksay: So in some countries you've already proceeded to delete the data on recommendations of privacy commissioners, but the Canadian data hasn't been deleted yet—I'm not understanding why—even though we have a recommendation from our Privacy Commissioner that it be deleted immediately.

Mr. Jacob Glick: I understood the "immediately" in that report to mean at the issuance of her final report.

Mr. Bill Siksay: Are you the one doing the analysis of her report, Mr. Glick, or is Dr. Whitten doing the analysis of that?

Mr. Jacob Glick: There are a number of people who are doing that analysis, and I'm certainly going to be involved in providing that analysis.

Mr. Bill Siksay: It seems to me that "immediately" means immediately, not February immediately, so it would be good to know the answer from Google on that specific question.

The Chair: Mr. Siksay, your time is up.

Go ahead, sir, and answer the question.

Mr. Jacob Glick: Thank you, Mr. Chair.

Just to be clear on the member's question, as I said in my opening statement, we don't want to have this data. If I have misunderstood the commissioner, then I apologize, and we're going to get on that.

That's the answer.

The Chair: Thank you, Mr. Siksay.

Mr. Poilievre, for seven minutes.

Mr. Pierre Poilievre: Thank you, Mr. Glick, for being with us today.

Just so we can retrace the steps in a *Coles Notes* fashion, you discovered through an audit that Google had inadvertently acquired payload data it had not intended to acquire.

● (1605)

Mr. Jacob Glick: That's correct.

Mr. Pierre Poilievre: Upon that discovery it reported this error to the privacy commissioners of the countries in which it operates. Is that correct?

Mr. Jacob Glick: We reported to the privacy commissioners in countries affected by this mistaken collection of data.

Mr. Pierre Poilievre: Could you just quickly rename those countries?

Mr. Jacob Glick: It would be the countries in which Street View is available. I don't know all of them off the top of my head.

Mr. Pierre Poilievre: Okay. I imagine it would be dozens of countries.

Mr. Jacob Glick: It would be the U.S., the U.K., Canada, Ireland, Australia....

Mr. Pierre Poilievre: How long after notifying them did you make this information public—not the information, not the data, but rather the existence of an error?

Mr. Jacob Glick: It was within days.

Mr. Pierre Poilievre: Based on the sequence of events I've read in the news and seen reported elsewhere, it would seem a mistake was inadvertently, unintentionally, made, but upon the discovery of that mistake Google immediately took responsibility and informed the relevant authorities and made the public aware.

Mr. Jacob Glick: That's correct.

Mr. Pierre Poilievre: It has since committed to solve the problem by destroying data it did not intend to have.

Mr. Jacob Glick: That's correct.

Mr. Pierre Poilievre: It sounds as if those are the kinds of steps a company should take in the event it discovers an error of this kind, and I congratulate Google for having taken public responsibility and quickly seeking a solution to the problem.

Just so we can more broadly educate the public on the nature of their own privacy in this digital age, what kind of information would be in payload data? For example, I understand the data was never transformed into humanly usable data for Google, but presuming that someone else had that data, would they be able to read private e-mails that were sent over the network?

Mr. Jacob Glick: This is a very good question and a helpful opportunity to provide a bit more technical elaboration, so thank you.

The short answer is—the commissioners, investigators, described this a bit last time, but I'll reiterate—the software was designed to flip channels five times a second. There are 11 different Wi-Fi channels and the software is designed to flip channels five times a second, so the cars are driving down the street and five times a second they're flipping channels, sampling payload data. The data that would get collected in that context would be highly fragmented; that is, only a snippet of information being sent at a particular moment in time would be collected.

Statistically—

Mr. Pierre Poilievre: Would that mean, for example, if I sent my e-mail at the exact moment when the Google vehicle was in range of my network, it might intercept and collect all or part of my e-mail during one of those fifth of a second channel changes?

Mr. Jacob Glick: The Privacy Commissioner's investigation found that, and we accept that as their finding. Statistically you would expect that it might happen in these circumstances, and we accept that those fragments of data collected can contain personal information.

Mr. Pierre Poilievre: Right. I say this not to pour vinegar on the wound, because I do understand the desire by Google to fix this. What I'm trying to get at here is the broader privacy problem for Canadians in the event there are actors in the world who have nefarious reasons for intercepting our private information. Obviously, with Google that is not the intention here. No one has suggested Google's intentions were anything untoward whatsoever, and that's not what I'm suggesting, but if other individuals had technology at their fingertips to intercept data travelling between networks, is this something Canadians need to be concerned about, or is it a stretch to suggest that could potentially occur?

● (1610)

Mr. Jacob Glick: I think this is something Canadians genuinely ought to be taking steps to protect themselves from, and there are important steps that every single Canadian can take to protect themselves and their data. I can name two for you.

Mr. Pierre Poilievre: Please.

Mr. Jacob Glick: The first is, if you have a home Wi-Fi router, put a password on it.

Mr. Pierre Poilievre: Okay.

Mr. Jacob Glick: That effectively puts encryption on your network, which means that the data travelling back and forth is gibberish. No one can read it unless they have a quantum computer. I'm being facetious. I'm not aware of the existence of a quantum computer that can break encryption, I should add.

Mr. Pierre Poilievre: On that point, before you go on to your second suggestion for Canadians, was the payload data you collected only from unsecured networks? They would have been instances in which people had failed to put on passwords. Is that correct?

Mr. Jacob Glick: That's correct.

Mr. Pierre Poilievre: For those of us who have passwords on our home Wi-Fi, if you had driven by and taken your five impressions per second, you would not have been able to intercept my e-mail, for example, as someone who has a password-protected Wi-Fi in my home. Is that correct?

Mr. Jacob Glick: Precisely.

Mr. Pierre Poilievre: Okay. So that is a good, practical suggestion.

You said you had a second one.

Mr. Jacob Glick: This is where the market comes in. Canadians should choose services that have encryption built into them. There are, for example, a number of different web mail products. To my knowledge, Google's Gmail is the only major web mail service that has encrypted connections built into it. So if you use Gmail, every time you connect, by default your connection is encrypted. Even if you're connecting over an unsecured network, your connection via Gmail is secure. Google has invested the time and the money into building encryption into its products. This is where the market can be helpful, because Canadians should choose products and services that have encryption built into them.

The Chair: Thank you very much, Mr. Poilievre.

Thank you, Mr. Glick.

That concludes the first round, colleagues. Now we'll start the second round, for five minutes each.

Ms. Bennett, we'll start with you for five minutes.

Hon. Carolyn Bennett: Thank you.

To follow up on my colleague's question, if you do Google “payload.data”, the first item that comes up is the Wikipedia definition; the second is the Whatis.com, and the third is the Google apology “Says Failed Badly” from May 18, 2010.

When we look at what you've said is obviously an inadvertent collection, and that this was back to some code that was written in 2006, and the code was written only to collect where the Wi-Fi signals were coming from, my concern is that this engineer who wrote the code....

My first question is, is that engineer still working at Google?

Mr. Jacob Glick: I cannot, unfortunately, comment on a personnel matter.

Hon. Carolyn Bennett: Okay.

The fact that this engineer took upon himself or herself to say that they didn't think it was a substantial privacy concern makes it sound as though you're now putting in place privacy training, as the Privacy Commissioner has asked, and to put somebody in charge who is the person...in most organizations to know what you know, know what you don't know, know who and when to ask for help. This person would, if any other engineer wasn't sure if there was a substantial privacy concern, immediately know who to ask.

Mr. Jacob Glick: That's right. Thank you for the question. You've got it exactly, which is that we want engineers themselves to be knowledgeable and accountable for the products they create.

In addition to that, though—and this is important—we are building additional checks and balances into the system, so that even if somebody makes a mistake or an error in judgment, that doesn't percolate all the way through to launch.

There were opportunities for this to be caught, but we want to build more opportunities, deeper opportunities. Included in the changes that we've announced, for example, are compliance audits, where there will be teams at Google whose job it is to audit the products that teams create to ensure that the actual thing that's happening is what's in the product design documents.

● (1615)

Hon. Carolyn Bennett: Is that a spot check, or is it in the process for developing a product that there is an automatic compliance audit for the new product?

The other piece of this is that the Privacy Commissioner has said that she will only consider the matter resolved upon receiving the evidence by February 1, 2011. It seems that the training issue is huge, so would the report that you send to her—so that she will be able to determine that her report is complete and so that she can make her final report and conclusions—include privacy training manuals and the kinds of protocols that will be put in place?

I don't necessarily expect you to share the Google training manual with this committee, but I am interested as to whether the training for engineers, and for all of the employees at Google, would be shared with the commissioner at that time.

Mr. Jacob Glick: The answer is that I don't know what the communication to the commissioner is going to be at that time, but I can tell you that we're working hard to have a full answer so that she can consider this matter resolved.

I should say that I've talked directly to Dr. Whitten precisely on this issue in the last week, and she's working flat out to try to implement the changes we've announced so that we can come back to the commissioner with not just announcements but real, substantive changes.

Hon. Carolyn Bennett: If someone is caught designing something or writing code for something that is not in compliance with the code or the interpretation of what is and is not a substantial privacy concern, which was the basis for this error, would there be, including in the manual, some consequences for somebody deeming something inconsequential without asking the new person in charge? Would you be able to share with the commissioner the consequences for not having asked and then for having written code that clearly is in violation of anybody's interpretation of privacy?

Mr. Jacob Glick: I think the key here is not the kinds of punitive measures that get put into place from an HR perspective, but rather the total system of compliance and checks and balances that gets created. At the end of the day, it's about Canadians. Resolving this matter is about the commissioner, but at the end of the day, it's about Canadians. It's so that Canadians can rest assured that their personal information is private and secure. It's ultimately our users who rely on trusting us with their data, because we know that our services are one click away from our competitors' services.

Hon. Carolyn Bennett: This is the code of conduct that you expect from now on.

The Chair: Ms. Bennett, your time is up.

Mr. Glick, I want to follow up with something, just to clarify.

Ms. Bennett asked whether the engineer who designed this program is still with Google. You have no reason to deny that information to a parliamentary committee. Maybe you don't know it, and you'll have to get back to us, but I'm directing you to answer that question.

Mr. Jacob Glick: I don't feel comfortable answering a personnel question. Can I take it under advisement?

The Chair: She didn't ask for his name; she just asked if he's still working for Google. It's a legitimate question for a parliamentary committee.

Mr. Jacob Glick: To my—

Mr. Harold Albrecht (Kitchener—Conestoga, CPC): Mr. Chair, I have a point of order.

I do think that personnel issues, generally speaking, even in parliamentary committees, are considered to be subject to being taken in camera. With due respect, I disagree with your statement.

The Chair: If you want to challenge the ruling of the chair, you can do it if you wish.

Mr. Harold Albrecht: I disagree.

The Chair: Are you challenging? Is that what you want to do?

Mr. Harold Albrecht: Mr. Chair, I just said that I disagree with your statement that a public witness would be mandated to divulge private information about company matters in a public session.

The Chair: Well, the chair has ruled. If you want to challenge the chair, that's certainly within your rights. This is an issue that caused a worldwide problem in Italy, in Germany, in the United States, and in Canada. I think it was a legitimate question.

You may not know the answer. We'll give you time to get back to us, but you certainly have no legal right to withhold that information from a parliamentary committee.

Mr. Jacob Glick: The answer is that I actually don't know the answer.

● (1620)

The Chair: That's fine. You can get back to us.

We're not looking for his name or where he works; we just want to know if he's still with Google. That was the question.

Mr. Jacob Glick: So when I—

The Chair: Or “she”. I'm sorry, it could be a “she”.

Mr. Jacob Glick: I'm not 100% sure.

The Chair: Okay, but you'll follow up and get back to the clerk of the committee on that point.

Mr. Jacob Glick: If I'm instructed by a parliamentary committee to do something, then I'm going to do it, I guess. I will consult with our external lawyers on this, because there could be all sorts of reasons why we may or may not be able to disclose it. But I understand the point you're making.

The Chair: It's certainly within your rights to consult whatever lawyers you want, but the order emanating from this committee is to provide us the answer in due course.

Mr. Jacob Glick: Understood.

The Chair: Ms. Davidson, five minutes.

Mrs. Patricia Davidson (Sarnia—Lambton, CPC): Thanks, Mr. Chair.

Thanks for being with us today, Mr. Glick. Certainly, we've had a fair amount of discussion about this.

There's one thing I want you to clarify before I ask you a question. You talked about three items you'd implemented in October or announced in October. One was the appointment of Dr. Whitten. One was “new safeguards with internal audits”. What was the third one? I missed that.

Mr. Jacob Glick: The third one was increased privacy training for all engineering staff. It's also for staff throughout the company, but in particular for engineers. If it's interesting for the committee, I've already had some preliminary discussions and my colleagues have had some preliminary discussions with some of the provincial privacy commissioners here in Canada who are interested in coming to Google and speaking to our engineers.

So back to the answer I provided to one of your colleagues, there isn't a particularly parochial view of privacy provided. A Canadian perspective of what “privacy” means gets provided and absorbed by our engineers globally. So we're working to make that a deep and meaningful experience that has a global impact.

Mrs. Patricia Davidson: Thank you.

This week, a friend of mine who is a Gmail subscriber received a message from Google that started out by saying that Google rarely contacts Gmail users via e-mail but they were making an exception to let them know that they'd reached a settlement in a lawsuit in the United States, I believe, regarding Google Buzz. It went on to say the settlement acknowledged this, and blah, blah, blah...and it was a mandatory announcement sent to all Gmail users in the States as part of that legal settlement.

What's being done with those same people who are Canadian users? My understanding is that they were automatically subject to the Buzz application, and unless they physically went in and reset their privacy settings, their privacy information could have been in jeopardy of being viewed by other Google Buzz users as well. The person who approached me about this had gone in and physically reset their privacy settings, but what about people who didn't do that? Are they in jeopardy of having their information accessed by other Google Buzz users?

Mr. Jacob Glick: No.

Mrs. Patricia Davidson: So why was this one person...?

Mr. Jacob Glick: I gave you a curt answer; I apologize.

I can go into a bit more detail about Google Buzz. The best way to describe it is kind of taking the functionality of Twitter, public updates—or private updates for that matter—and integrating that into Gmail. The way that was launched provided some very negative feedback from our users and resulted in lawsuits. By the way, we changed the launch procedure within 48 hours of the launch of the product, realizing we'd upset people. We didn't, though, disclose people's personal information without their consent. The product had a bad user experience, though, at launch, and we corrected that immediately because of an outcry from our users. This is similar to what I've described before, which is that we are attentive to what our users care about and we want them to like the products, and when they don't like a product we want to fix that.

Mrs. Patricia Davidson: So a Canadian user, then, on Google Buzz, whether or not they went in and reset privacy settings, was at no risk of having privacy issues violated. Is that correct?

● (1625)

Mr. Jacob Glick: The short answer is no. The long answer is that it's going to take more time than we have to explain, but I'd be happy to meet with you to describe in more depth how Buzz works, what it is, and what the concern is.

But the short answer is no, Canadians' personal information is not at risk.

Mrs. Patricia Davidson: So they don't need to be concerned about going in and resetting their privacy settings?

Mr. Jacob Glick: To be clear, if they don't want to use Google Buzz, then they have no reason to be signed up for it, and there's a way in their settings to just turn it off and get rid of it. So if they don't want to use Google Buzz, there's an easy way to get rid of it, and if—

Mrs. Patricia Davidson: I understood they're automatically subject to the Buzz application, whether they signed up for it or not, that if they had a Gmail account, they were automatically subject to it. That is what I was told.

Mr. Jacob Glick: That's not correct. What happened was that every Gmail user was given the opportunity to join this additional service, which was built into Gmail, but it was not obligatory that people sign up for it.

The Chair: Just a short question.

Mrs. Patricia Davidson: So it was not a reverse registration, if you want to call it that, or a reverse sign-up, where you were automatically signed up unless you physically did not sign up?

Mr. Jacob Glick: That's right.

There were a number of interstitials that users had to go through in order to get access to Google Buzz and start using it. But different users didn't like that sign-up process, in any event—which we changed.

The Chair: Thank you, Ms. Davidson.

Monsieur Nadeau, *pour cinq minutes*.

[*Translation*]

Mr. Richard Nadeau: Thank you, Chair.

Mr. Glick, in Canada, how extensive is the coverage by street level imaging?

[*English*]

Mr. Jacob Glick: We have a significant portion of the country mapped. The way to see it is by going to Google Maps and finding the little "peg man", as we call him. I don't make up these names; I just repeat them at committee. You drag "peg man" over the map and all of the places that are covered in Street View will light up as blue.

But the answer is that we have mapped most communities throughout Canada, large and small, because we believe that everyone should have the opportunity of accessing next-generation maps.

[*Translation*]

Mr. Richard Nadeau: That is what you believe.

Otherwise, I presume there must be an update after a while.

In cities, the population changes, frontiers move one way or the other because of new construction, or neighbourhoods are remodelled. Did you make a decision that images will be valid for five years and then you will have to go back to these same places?

How does it work?

[*English*]

Mr. Jacob Glick: That's a great question. Thank you.

The short answer to your question is that there's no particular timeline, but with your indulgence, I have an interesting anecdote for you that provides a bit of colour to this.

During the last collection of data we photographed the city of Windsor, unfortunately, during their garbage strike. The city fathers were a little disappointed that the image they were presenting to the world was of a city with garbage piled up everywhere, and they actually wrote to Google and the correspondence was directed to me, specifically, saying, "Please, come back to Windsor. We want you to come back and photograph Windsor when there isn't garbage piled up everywhere." So we in fact did do that. We came back to Windsor specifically to photograph it again.

I should also say that Toronto was partially photographed during their garbage strike. So if you go to Google Maps, you will see that Christie Pits Park had a whole bunch of garbage piled up in it. Toronto hasn't requested that we come back, but we did go back to Windsor because it was important to the people of Windsor that the Google cars return and a clean vision of the city be presented.

[*Translation*]

Mr. Richard Nadeau: If I am not mistaken, Toronto has a new mayor, and there will not be any trash cans in the streets ever. The matter is settled.

Mr. Jacob Glick: Ah, ah!

Mr. Richard Nadeau: That being said, I am very much interested in one thing, and that is the technology you are using, and about which we have been talking for a while, to get the imagery and blur faces, licence plates on cars and street numbers on houses. Once you get all the material, it must be a painstaking work you have to do in order to sort out all this information

Technology is changing fast. Do you upgrade your software in order to protect people's security or at least their privacy? How do you do it? Are you choosing the newer technologies or do you keep the same blurring technique?

● (1630)

[*English*]

Mr. Jacob Glick: Again, it's an excellent question.

The facial recognition technology we use is literally the most sophisticated in the world. We developed it precisely so we could protect people's privacy.

It's funny, because you can go into Best Buy or Costco and get a camera that shows where all the faces are when you look in it, so you think this is trivial technology. This is again where I go on what I've been told; this is not my own area of expertise. As I understand it, that's about 90% accurate, and it is a trivial technical matter to have 90% accuracy in terms of figuring out where the faces are. From 90% to 95% is really hard, and 95%-plus is one of the hardest computer science challenges in the world. That's where we are in terms of the accuracy of facial recognition for the purposes of blurring.

Our engineers have published scientific papers on this. We were written up in *The Economist* recently as one of the best examples of machine learning and how machine learning can be used for important purposes like privacy protection. We are constantly innovating on technologies like this.

[*Translation*]

The Chair: Thank you, Mr. Nadeau.

[*English*]

Mr. Albrecht, five minutes.

Mr. Harold Albrecht: Thank you, Mr. Chair.

Thank you, Mr. Glick, for being here today.

I really want to applaud you for your forthright testimony today. I think your admissions have been refreshing, understanding the fact it was an inadvertent error and that you're taking all necessary steps to correct the matter, from what I can tell.

I was surprised to hear about the number of Canadians who are using Street View. I think that indicates the value of Street View. You indicated that possibly it's especially valuable for those who can't read maps. I would suggest it's also valuable for anybody from Kitchener, because Kitchener has a series of streets that run in many different directions, as you would know, coming from that area. King Street runs east, west, north, and south, so it's difficult to give someone directions. So I appreciate your efforts there.

I'm disappointed that you don't have many of the rural areas mapped on Street View. I also represent three townships: Wellesley, Wilmot, and Woolwich. It's disappointing that I can't take a Sunday afternoon drive on Google and see the beautiful landscape in my riding. That's just a little bit of encouragement for you to get the rural areas up as well. Maybe there are initiatives to do the rural areas. My use of Street View has been very limited, so I'm not sure if many of the rural areas are covered. Are they?

Mr. Jacob Glick: Yes, rural areas across the country have been covered. I don't know about those areas in particular. As soon as I go home I'm going to see if—

Mr. Harold Albrecht: We're going to get those done.

Mr. Jacob Glick: —New Dundee and Elora and Elmira and St. Jacobs and Fergus, all those communities, are up there.

Mr. Harold Albrecht: I'll provide you with a Google map to get you around.

Mr. Jacob Glick: Yes.

Mr. Harold Albrecht: On a more serious note, you mentioned the training aspect of what you want to do to increase the level of confidence Canadians can have in privacy issues. The other concern the Privacy Commissioner raised to us was not only the training but the actual incorporation in the development stage of technology so that these issues are addressed beforehand in a proactive manner as opposed to a reactive manner. I'd like you to respond to that.

A second part to that question.... I know you have offices in Waterloo, which I understand are being moved to Kitchener, and you have a number of employees there. Are you finding it difficult to find people who have the technical qualifications you would need in an application like we're discussing today?

● (1635)

Mr. Jacob Glick: Thanks very much for the questions. I'll answer them in reverse order, if you don't mind, just for the committee's benefit.

We are looking for, literally, the top engineering minds in Canada, and we're attracting them because of what a quality place it is to work. Frankly, it is really hard for Google in general to find people, but as the Waterloo office goes on a global basis for Google, they've had particular success because of the top-quality education system we have and the top-quality engineering minds we have.

On the other question you've asked, about what the commissioner referred to as privacy by design—and this is a term coined by Ontario privacy commissioner Ann Cavoukian—we are very supportive of the principles that Commissioner Cavoukian has been evangelizing, which is to really bring the values of privacy deeply into an organization, from the start of the product design process.

If you think about it, we were talking a little bit before about how encryption is built into Gmail: that's privacy by design. Commissioner Cavoukian has said that previously. That's privacy by design because built right into the product is a key privacy protection that makes sure you and Google have a private communication, that no one else is getting in there.

So we want to continue to be able to do things like that. The education we're providing is I hope going to deepen those kinds of efforts within the company.

Mr. Harold Albrecht: Thank you very much.

The Chair: Thank you, Mr. Albrecht.

Mr. Siksay for four minutes, and then we have to let the witness go.

Mr. Bill Siksay: Thank you, Chair.

Mr. Glick, you know I'm an enthusiastic supporter of Google and Google Street View, in particular. I'm a constant user of it, and I'm very happy with what Google did to meet the privacy concerns around the rollout and operation of Street View. I have no questions about that. I think that's been great.

I think that's why I'm so disappointed in what's happened in terms of the extra information that was collected during that process, that nobody knew about, and I still have some questions about that. We were talking about the deleting of the payload data. I want to know if you know of any impediment under U.S. law to the deletion of that information, the Canadian data.

Mr. Jacob Glick: I'm not a U.S. lawyer, so I wouldn't speculate.

Mr. Bill Siksay: Do you know if Google has identified any impediment to that?

Mr. Jacob Glick: I'm not aware of anything, but again, this is going to be part of the process that we go through as soon as I leave this room and call—

Mr. Bill Siksay: If you could let us know the answer to that, it would be very helpful.

Do you know if—

The Chair: If you would get back to the committee with that information, that would—

Mr. Bill Siksay: That would be great.

The Chair: Obviously, he doesn't know it now.

Mr. Jacob Glick: Again, Mr. Chair, if we go through this process and determine that we can delete it asap, and that's what the commissioner wants, we'll go ahead and do that and we'll advise the committee that we've done that.

Mr. Bill Siksay: The commissioner's report does say on or before February 1, so I don't think you have to wait till February 1 to do any of this, Mr. Glick.

Mr. Jacob Glick: Right.

Mr. Bill Siksay: Would Dr. Whitten be available to appear before the committee?

Mr. Jacob Glick: I don't see any inherent problem with that. It all depends on availability. In this case in particular, for example, the committee wanted to hear from Google on very short notice, and it was important to us to appear because we wanted to be able to answer your questions.

Mr. Bill Siksay: I do appreciate that you're here and I know you have limited time.

I want to ask some specific questions. For me there's the Street View, street imaging, mapping, cartography, photographic process. There's the payload data download. There's also the collection of Wi-Fi hotspots. I think the commissioner is working on the payload data issue with Google now, but I'm concerned about the Wi-Fi hotspots. Folks from the commissioner's office did identify that there could be privacy concerns around that, and you've raised several things today that I want to ask you about.

You said that many companies have done the gathering of Wi-Fi hotspot data detection; they've done that process. It's not only Google. Do you know how many companies have done that?

Mr. Jacob Glick: I don't know the names of all the companies globally or in Canada who do that, but there are certainly quite a number of companies operating in Canada, at least that I'm aware of. By the way, there's a way that this could be done through what's called crowd-sourced data. If you Google public Wi-Fi hotspots, one of the first sites you get is a map that people have created themselves, based on publicly available software that does I think something similar, which is that you open it up on your computer and you can drive around and create and upload it to a public database and you can make that available. That data can be licensed by other companies.

● (1640)

Mr. Bill Siksay: The technology that Google used to collect these Wi-Fi hotspots, was that their own technology developed by Google?

Mr. Jacob Glick: I think it's based on well understood practices in the industry. How this is done, I don't—

Mr. Bill Siksay: But the actual program that did it, was it a Google program?

Mr. Jacob Glick: It was a program written by a Google engineer, but I think it was based on an open-source program.

Mr. Bill Siksay: Has Google shared that program with other companies, do you know? Is it something that you've commercialized in any way?

Mr. Jacob Glick: Well, the open-source software is publicly available and you could download it in your office later today. In terms of the specific code at issue that collected the payload data, that code was examined by third-party auditors, and their report is available on our blog. We've made that report, as I think I mentioned in my remarks, available to the commissioner as part of her investigation.

The Chair: Mr. Siksay, I'm going to interrupt you. I think the witness has to catch a plane, so we're going to—

Mr. Bill Siksay: Chair, point of order.

Chair, I do have other questions for Google, so I wonder if we could arrange for Mr. Glick, or perhaps Dr. Whitten, to appear before the committee at some point.

The Chair: That's something you could bring to the steering committee.

Mr. Glick is here in Ottawa, so it won't be a large imposition for him to come back before the committee.

I understand that you have a flight to catch, so we're going to suspend this part of the meeting. We have other committee business, but on behalf of all members of the committee, I thank you very much for your attendance here today.

If you have any brief closing remarks—if you don't, it's fine—but if you have anything you want to say....

I understand the analysts may be in touch with you regarding some technical issues but non-evidentiary. They will deal directly with you, sir.

Do you have any closing comments?

Mr. Jacob Glick: I'll just say thank you, Mr. Chair, for having me here today, and thank you to the members of the committee for your thoughtful questions.

The Chair: Thank you very much for your appearance.

We will suspend for 30 seconds and we'll come back in camera.

[*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