House of Commons
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 034 • 3rd SESSION • 40th PARLIAMENT

EVIDENCE

Thursday, November 25, 2010

Chair

The Honourable Shawn Murphy

Standing Committee on Access to Information, Privacy and Ethics

Thursday, November 25, 2010

● (1530)

[*English*]

The Chair (Hon. Shawn Murphy (Charlottetown, Lib.)): It being 3:30 p.m., I will call the meeting to order and extend to everyone here a warm welcome.

This meeting has been called pursuant to the Standing Orders and is our last meeting to deal with witnesses on our study of the street-imaging applications Google, Canpages, etc. The committee has before it four witnesses today. Two of them are coming to us through video conference.

We have Mr. Jacob Glick, Canadian policy counsel with Google Inc. He is joining us from Toronto via telephone conference. We're also joined by Alma Whitten, who is the engineering lead for privacy for the worldwide Google organization. She also is joining us via telephone conference, from London, England.

In addition, we have two officials from the Yellow Pages Group Co., which recently, I understand, purchased the Canpages operation. We have François Ramsay, senior vice-president, general counsel, and secretary responsible for privacy, and Martin Aubut, senior manager for social commerce.

I want to welcome everyone here to the meeting, but before we ask for any opening remarks, I want to ensure that our technology is working.

Mr. Glick, are you on the line? Can you hear me?

Mr. Jacob Glick (Canada Policy Counsel, Google Inc.): I can hear you and I can see you a little bit. The audio is fine. The screen is flickering quite a bit in terms of the video.

The Chair: We can hear you reasonably well. You're seeing me okay? I'll keep my head still, maybe they can get it.

Dr. Whitten, can you see and hear me?

Dr. Alma Whitten (Engineering Lead for Privacy, Google Inc.): I have the same experience as Mr. Glick. I can hear you very, very well, but my screen image is jumping around quite a bit.

The Chair: Yes, we can see that. That is a technological problem, but we'll just continue with it and hope it won't annoy you too much; you're looking at the whole thing and I know it would be somewhat annoying.

First of all, I will invite Mr. Ramsay to give his opening comments and then I'm going to ask Dr. Whitten or Mr. Glick if they have any opening comments.

Mr. Ramsay.

Mr. François Ramsay (Senior Vice-President, General Counsel, Secretary and Responsible for Privacy, Yellow Pages Group Co.): Thank you, Mr. Chairman.

Thank you for inviting us to the committee. It is a pleasure to appear in front of you.

With me this afternoon is Martin Aubut, who is senior manager, social commerce, of the Yellow Pages Group. Martin is an expert on the Internet. I thought having him with me today could be useful should your questions touch on issues that I am less familiar with.

In addition to my responsibilities as general counsel of Yellow Media Inc., the ultimate parent company of Canpages and Yellow Pages Group, I am the acting privacy officer of the company.

I thought I would start by giving you a brief introduction of Yellow Pages Group, also known as YPG, which acquired Canpages in June 2010.

Yellow Media Inc. is a leading Internet company in our network of companies, which includes Yellow Pages Group, Trader Corporation, and Canpages. Yellow Media owns and operates some of Canada's leading properties and publications, including Yellow Pages directories, YellowPages.ca, Canada411.ca, AutoTrader.ca, CanadianDriver.com, RedFlagDeals.com, and LesPAC.com.

Our online destinations reach over 11.5 million visitors monthly, and our mobile applications for finding local businesses, deals, and vehicles have been downloaded over two million times. We're also a leader in national digital advertising through Mediative, a provider of digital advertising and marketing solutions to national agencies and advertisers.

Predecessors of YPG published their first directories in 1908. We have operations in all the provinces and territories of Canada. There are approximately 2,500 employees at YPG, 530 at Canpages, and 1,200 at Trader.

Through the acquisition of Canpages, we hope to be in a better position to compete with other major online players such as Google. We believe that our acquisition of Canpages will sharpen our online competitiveness by expanding our sales force, capabilities, and offerings, thus accelerating our move online.

If you factor in the sales professionals we have at YPG, Trader, and Canpages, we have approximately 2,000 people in the sales organization. We're looking at a better utilization of that tremendous sales capacity, targeted at small and medium-sized Canadian enterprises.

You should know that Street View, the service currently offered on Canpages.ca, is licensed from two third parties, one of which is MapJack, for parts of the cities of Vancouver, Toronto, and Montreal. Street View has been in effect since 2008; Google Street View is used for the rest of Canada.

Depending on where you are within our universe of websites, we are currently using Street View technology from Google and Microsoft, in addition to MapJack, the provider that Canpages has historically used.

I am pleased to confirm to the committee that Canpages' supplier of the Street Scene service, MapJack, has not been used to collect either Wi-Fi network data or Wi-Fi payload data. Therefore, we have never been in possession of any such data.

Yellow Media Inc., YPG, Trader, and Canpages are fully committed to abiding by the privacy legislation applicable to our business.

We would be pleased to answer any questions the committee may have.

Thank you.

● (1535)

The Chair: Thank you, Mr. Ramsay.

Mr. Glick, do you have any opening comments to make to the committee?

Mr. Jacob Glick: No, Mr. Chair. I will only thank the committee for having us back and will give the floor to Dr. Whitten, who I think has some remarks.

The Chair: Dr. Whitten, if you have any opening remarks to make, I invite you to do so now.

Dr. Alma Whitten: Thank you to the committee chair and to all the members of the committee for this opportunity to speak with you today.

I've devoted my career both as an academic and now as Google's director of privacy to one primary goal, which is to make it intuitive, simple, and useful for Internet users to take control of their privacy and security.

This is really the central challenge of privacy engineering. Products and services, particularly on the Internet, constantly evolve. Valuable new services, from social networking to online video to mobile computing, are constantly changing the way in which we interact with each other and use information.

These services, which are built in part from the information that providers learn from their users, offer tremendous value. Our goal is to offer our users innovative products that help them understand the world in new and exciting ways.

In order to do what we do, in order to provide great user experiences, we rely on our users' trust. It is our greatest asset. The information our users entrust to us enables us to better match searchers to the information they seek, to fight off those who would scam our users or undermine the usefulness of our search results, and to create new services, such as translation, speech-to-text, and many others.

We focus on building transparency, user control, and security into our products. We constantly review, innovate, and iterate to make sure we are honouring our users' privacy expectations and security needs. Because our users' trust is so critical to us, it's very important to us to note that we do not sell our users' personal information.

The Google Dashboard is a cornerstone of our efforts. If you haven't seen this tool, I invite you to take a look at www.google.com/dashboard. We developed the dashboard to provide users with a one-stop, easy-to-use control panel for the personal information associated with their Google accounts, from Gmail to Picasa to Search, and to more than 20 other Google products.

With the dashboard, a user can see, edit, and delete the data stored with her individual Google account. She can change her privacy settings, see what she is sharing and keeping private, and click into the settings for any individual product.

I was adamant when we created the dashboard that we not make it seem strictly a privacy tool. Above all, I wanted it to be a useful tool that our users would come back to and interact with even when they weren't consciously thinking about privacy.

We took a similar approach with our advertising network. Our ads preferences manager, which is linked from every ad in our advertising network, allows users to opt out of ad targeting and learn about our privacy practices. Equally important, it allows users to look at the categories of ads they will see, select new interest categories, and remove ones that don't match their interests.

By offering this useful service, we hope to get more people to understand and confirm their privacy settings. Interestingly, we have seen that for every one user who visits this page and opts out, four choose to edit their preferences, while ten view the page and choose to do nothing.

These are great examples of transparency and control designed into products in a way that is prompting individual users to learn more about how to control their information, and we're proud of this track record.

However, despite our best efforts, on occasion we have made mistakes. As this committee is well aware, in May, Google disclosed that we had mistakenly included code in the software on our Street View cars that collected samples of Wi-Fi payload data—information that was sent over open, unencrypted Wi-Fi networks. To be clear, Google never used this mistakenly collected data in any product or service, and there was no breach or disclosure of personal information to any third party. As soon as we learned about this incident, we disclosed what had happened and acknowledged our mistake.

Google is working hard to fully and completely address this incident. We recognize that we need to do better.

My colleague Jacob Glick spoke to you in November about some of our plans to strengthen our internal privacy and security practices. These plans include additional responsibilities for me, which I would appreciate telling you a bit about today.

● (1540)

I'm excited by the opportunity bring greater robustness to our privacy and security practices in my new role. With my expanded responsibilities, I will have the chance to oversee and work with both the engineering and the product teams to help ensure that privacy and security considerations are built into all of our products.

While the duties that go with this role are big, I am confident that I will be supported with the resources and internal support needed to help Google do better. Further, I believe that Google's commitment to redouble its efforts around staff training will go a long way.

Mr. Glick mentioned this when he appeared before this committee on November 4, and I'm happy to elaborate on this further for you. We want to deputize every Googler in this effort. We want to make certain that each product we roll out meets the high privacy and security standards that our users expect of us.

We are an innovative company, creating new products each year that are helping to transform how we organize information and relate to each other as people. Our users' trust is the foundation that Google's business is built upon. We are committed to not taking that trust for granted.

I look forward to answering your questions.

Thank you.

The Chair: Thank you very much, Dr. Whitten, for those remarks.

We're now going to start the first round.

Mr. Easter, you have seven minutes.

Mr. Bill Siksay (Burnaby—Douglas, NDP): I have a point of order, Chair.

The Chair: Mr. Siksay.

Mr. Bill Siksay: Chair, the clerk distributed a note from Mr. Glick prior to the meeting saying that he would update us on the matter of the deletion of Canadian data and the analysis of that information. I wonder if that might be part of the report that we hear from the Google folks before we go into questioning, since it was promised for this meeting.

The Chair: To follow up on that point, we did circulate a letter. I'll read it into the record. It was given to us in both official languages

On that point: “With respect to your question regarding any impediments under U.S. law to the deletion of the Canadian data, Google is working on analyzing the information and Jacob will give the committee an update on Thursday”. You just wanted an update on that point before you go into questioning, Mr. Siksay? Okay.

I'm going to come back to you, Mr. Glick, and I hope you've heard me. What the committee is looking for is for you to address that issue. Just to make it absolutely clear, we understand that you are prepared to give us an update—and I'll read this—“regarding any impediments under U.S. law to the deletion of the Canadian data”.

We understand that your company was analyzing this information and that you were going to give us an update here today. I'll ask you to address that issue now.

● (1545)

Mr. Jacob Glick: Sure. Thanks very much, Mr. Chair. I hope the members can hear me.

As you know, when we were at committee last time, we hadn't yet begun the analysis of what steps, if any, we could take to delete the data pursuant to the direction of the Privacy Commissioner. At that time, I promised that we would begin that analysis right away. We've begun that analysis; there's a process under way. It's not complete yet, but we hope to have a better understanding as this progresses.

I can tell you that the bottom line is the same as what I said it was last time we were here, which is that we want to be able to delete the data, but this is a difficult series of questions and something that we only get a chance to do once—that is, delete the data—so we want to make sure we do it right. There's a process under way to do that analysis, but it's not complete yet.

The Chair: When do you expect to have it completed?

Mr. Jacob Glick: I can't say for certain, but my expectation is that by the new year we'll have some much more definitive answers as to what data we can delete, if any.

As part of the process set in motion by the Privacy Commissioner, we'll be reporting back to her in accordance with her draft findings. Because it's a process that's ongoing, I can't tell you definitively, but we're moving quickly. It's just that it is difficult.

The Chair: I'm sure people will have questions on that issue.

We'll go to Mr. Easter for seven minutes.

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

First of all, thanks to all of you for appearing. Technology is amazing. When you can beam in somebody from England, times are changing.

For the Yellow Pages folks, as you're aware, we had Google people before the committee over what seems to be inadvertent collection of data about which there are privacy concerns, at least at this stage. I think you made it clear in your remarks that you've never been in a position to collect private data given the way you do collection of data and mapping. Is that what I'm hearing?

Mr. François Ramsay: Yes.

Hon. Wayne Easter: So what do you do differently to prevent that?

Mr. François Ramsay: The first thing you should understand is that, strictly speaking, Canpages—or Yellow Pages Group—is not in the business of doing street mapping the way other providers are. We use a third party to do that service. When Canpages started doing this service back in 2008, it used a company called MapJack. Before coming here today, we received assurances from this company in relation to the fact that they would have collected that kind of information. They've confirmed to us that they have not collected that information, and we don't have that information.

Hon. Wayne Easter: In our discussion when we had the Google folks before committee, it seemed that it was sometime after the data was collected that they learned there really had been an infringement of privacy. As you can tell from the discussion with Mr. Glick, Google is still trying to see whether it can be destroyed or not. How can you be absolutely sure when you're dealing with another company?

● (1550)

Mr. François Ramsay: I guess I can only repeat those assurances that I have received from the principals at MapJack. That being said, this company is based in Hong Kong, and my understanding of this company is that it's not a very large corporation. It was using technology that I think—and I guess maybe Martin needs to confirm—was much less sophisticated than the services offered or rolled out by Google and Microsoft.

What I can again repeat to the committee is the fact that these are the assurances we have received. The hosting of the mapping service of this technology is based here in Canada. We have the licence to use it here in Canada, but there is nothing other than the map services and the street scenes that we provide through the use of our websites.

Hon. Wayne Easter: I have one other question that I think it is something that committee members have pushed to other witnesses, and that is with regard to the controls in place in various companies to ensure there are procedures in place to protect privacy. The second part of that is really about what your company, Yellow Pages and its various subsidiaries, or the ones you've taken over, does to ensure compliance by your staff now and in the future as things change.

Mr. François Ramsay: We have put in place privacy policies that are posted on our websites and that users can access and review. We are currently reviewing these privacy policies to make them more uniform throughout the company, as the company has grown through acquisitions over the course of the past few years. We are satisfied that we are complying with privacy legislation as it exists.

As for the policies and the systems we have in place to ensure privacy—and maybe this is where, if the conversation becomes slightly more technical, I will have to pass the mike over to Martin—my understanding is that our IS/IT department has put in place systems that would be the accepted industry standards relative to protecting privacy. As far as receiving and dealing with privacy complaints is concerned, they all come through my office. To be very candid and very transparent in front of the committee, there are very limited instances where privacy concerns have been raised and have reached my office and we have had to deal with them.

Hon. Wayne Easter: Thank you, Mr. Ramsay.

My last question is to Ms. Whitten.

You talked fairly extensively about what I think you called the dashboard. You indicated that it's not strictly a privacy tool and that when it was designed you didn't want it to be strictly a privacy tool. I listened to your explanation, but could you explain to me, maybe in more detail, how this dashboard is in fact a privacy tool, how it protects privacy?

Dr. Alma Whitten: Certainly. I would be happy to.

Let me first clarify a bit about what I was getting at in saying that we didn't want it to be only a privacy tool. As my privacy team works to build privacy tools and to build transparency and control into all of Google's products, one of the things we're very aware of is that there's very often a valid critique that these settings and options for users are buried underneath a privacy link or a privacy option where nobody ever actually goes.

We wanted to be ambitious about addressing that problem by making the dashboard as much as possible a place where people would simply go to see all the information in their account for all kinds of reasons: because they're looking for something or because it's useful to them in other ways. By doing that, it would keep them informed about the information, about the data that was in all the different Google services they might have used over time.

It would keep them informed about which services they might have used at one time, then forgotten about and never gone back to again, but that still have some of their data. They would be informed in this way even if they never had that moment of thinking that they should check on their privacy. We felt that was a way for us to reach, to protect, and to better serve more of our users, even if they weren't necessarily people who were already very conscious of privacy as a question.

● (1555)

The Chair: Thank you, Mr. Easter.

Thank you, Dr. Whitten.

We're now going to move to Madame Thi Lac.

Madame Thi Lac, vous disposez de sept minutes.

[*Translation*]

Mrs. Ève-Mary Thaï Thi Lac (Saint-Hyacinthe—Bagot, BQ): Good afternoon, Ms. Whitten, Mr. Ramsay and Mr. Aubut. Good afternoon, Mr. Glick, giving your testimony today by videoconference.

My first question goes to Canpages.

You told my Liberal colleague that you had subcontracted your MapJack service, but the only guarantee you got was the one that your subcontractor was prepared to give you. As the one responsible for the service, how confident do you feel about that? Were you just given verbal assurances, or guarantees that really let you declare to the committee today that the service is secure?

Mr. François Ramsay: That is an excellent question and I hope that I will be able to put the committee at ease by providing it with some assurances.

I can tell you that Canpages, actually Yellow Pages Group Co., is not a highly developed technology company. Neither Canpages nor Yellow Pages Group Co. have the technology inside the company to produce a service like Street Scene or Street View.

When Olivier Vincent came to address the committee in June 2009, he explained, if I am not mistaken, that we were right at the start of services like Street Scene.

Against that background, Canpages still had the foresight to require confidentiality assurances from its supplier. If I am not mistaken, Mr. Vincent told the committee that the company had committed to destroy and discard any image in which things like vehicle licence plates and faces, I believe, had not been blurred.

Mrs. Ève-Mary Thaï Thi Lac: Mr. Ramsay, when you say that you required assurances, they are the ones we have already received as a committee, they do not give additional information that have already been provided to—

Mr. François Ramsay: Since we were invited to be part of the committee's work, and when we became aware of Google's testimony last November, we got in touch with the supplier and asked for clarification on the incidents that happened when Google was taking pictures. We then looked into whether comparable situations had arisen. Our supplier assured us that Wi-Fi zones had not been detected and that no data transmitted from those zones had been intercepted either. Basically, they did not have the technology to identify Wi-Fi zones in the street as the pictures were being taken.

Mrs. Ève-Mary Thaï Thi Lac: Thank you. I have a final question, but could you answer quickly because I'd like to have time to ask the people from Google some questions.

Can you tell us what technology MapJack uses to gather its information?

● (1600)

Mr. Martin Aubut (Senior Manager, Social Commerce, Yellow Pages Group Co.): Good afternoon. I do not have information about exactly which technology our supplier uses. What I want to add, as a follow-up to your first question, is that we just use the images; MapJack uses nothing else that could be considered other data. For us, it really is all about the image, a specific interaction at a specific point.

Mrs. Ève-Mary Thaï Thi Lac: Thank you very much.

Now I am going to talk to Ms. Whitten. You said that you are engaged in training your 23,000 employees on the protection of personal data and privacy. Can you tell us what that training consists of?

[*English*]

Dr. Alma Whitten: Certainly. The improved training that we are putting in place has a number of aspects.

First, we are going to have broad security and privacy compliance training and code of conduct compliance training across the entire company—both of those things for all of the employees.

Second, there is going to be a more focused and deeper training specific to different kinds of job roles. We are currently in the process of putting together a much more focused and in-depth training for engineers and product managers that will be specific to their jobs. We will also be looking at other functions within the company, such as legal functions and customer service and sales, to offer appropriate and more in-depth training for each of those roles.

[*Translation*]

Mrs. Ève-Mary Thaï Thi Lac: At the moment, you cannot state that the information and data gathered by accident on Google Street has all been deleted. But I see that Google has erased the data that was gathered accidentally in Great Britain. I have an article about that, dated last November 19, which is quite recently.

I would like to know why it was possible to destroy the information in Great Britain, but it has not been possible to do the same in Canada. My question goes to Mr. Glick.

[*English*]

Dr. Alma Whitten: I will answer in part, but then I will also invite Mr. Glick to answer specifically to Canada.

Everywhere, in every country where we have any of this data, it has always been Google's desire, since we discovered that we had mistakenly collected this data, to delete it as quickly as possible. In each country, we have been cooperating very closely with the appropriate data protection authorities as they investigate how this data came to be collected, and in each country when we have been able to establish that there is no legal requirement for us to keep the data, we have immediately moved to delete it.

I will ask Mr. Glick to also chime in to answer your question, because he is the specialist for Canada.

Mr. Jacob Glick: Thank you very much.

First, I think I said in my remarks to the committee on November 4 that we had deleted the U.K. data. I actually am not sure that this is the case. I misspoke when I said that, because I thought that the investigation had been concluded. In fact, it concluded subsequent to my appearance.

I'm not certain that the data has been deleted. I just don't know the answer to that. But the analysis that's being undertaken in the U.K. will be similar to what's happening in Canada and elsewhere in the world. We want to confirm all of the obligations we have under relevant law to preserve data so as to ensure that in the process of deleting it we don't inadvertently do something else that's bad.

Again, this is what I mentioned in response to the committee's question and to the point Mr. Siksay raised, which is that we only get one chance to delete the data. The analysis has to be incredibly thorough to ensure that we get it right.

● (1605)

[*Translation*]

Mrs. Ève-Mary Thaï Thi Lac: Thank you very much.

[*English*]

The Chair: *Merci.*

Mr. Siksay, you have seven minutes.

Mr. Bill Siksay: Thank you, Mr. Chair.

I want to thank the gentlemen from Canpages and the Yellow Pages Group for being here today, as well as Mr. Glick and Dr. Whitten.

Dr. Whitten, thank you for staying up late and working late to be with us today.

My questions are probably for Mr. Glick and Dr. Whitten.

Mr. Glick, can you tell us exactly where the payload data that was captured in Canada is currently being stored?

Mr. Jacob Glick: It's being stored in a secure facility in California, the same place it's been stored in since the Privacy Commissioner's investigators reviewed it.

Mr. Bill Siksay: You can confirm that the data is actually held in California? Because I think the Privacy Commissioner's folks weren't sure that it was actually at the Google headquarters in California or that it may have been held somewhere else. Your information is that it is held in California.

Mr. Jacob Glick: As far as I know, it's in a secure facility there. I don't know that it's on the Google campus. I think it's being held by a third party, but I'm not 100% certain about that. Dr. Whitten may have some additional information.

Wherever it was being stored at the time that the Privacy Commissioner's investigators came to review it is the same place it's being stored today, in a secure manner. It is segregated from the Google corporate network and segregated from any other data, and there is limited access to it. All of the security restrictions in place that were around the data when her investigators came to review it are in place today.

Mr. Bill Siksay: You can confirm that it's not being stored in Canada. The information has left Canada and is being stored in the United States?

Mr. Jacob Glick: Well, it left Canada when it was collected in the cars. So it's not like it left Canada during the process of this investigation.

Mr. Bill Siksay: Right. I understand that. So my question—and maybe, Mr. Glick, you can help me with this—is what the legal issues are that require analysis in this case. Is this about conforming with U.S. law? Since this Canadian data, this information that relates to Canadians, is being held offshore, in the United States, is the analysis about what American law we have to comply with?

I ask that question especially given that the Privacy Commissioner of Canada has recommended the immediate destruction of this data. Are there legal issues that Google is currently analyzing? Can you tell me what those are? Also, do they relate to the fact that information about Canadians is being held in the United States?

Mr. Jacob Glick: Just to be clear on what the Privacy Commissioner said, she raises this issue twice in her report, in paragraph 69, and then in her recommendations in paragraph 72. In paragraph 69, she says: “To this, I would like to add that not only privacy laws, but other applicable laws in the U.S. and in Canada, including laws of evidence, must also be taken into account in determining when to delete the Canadian payload data collected”.

Then she goes on to say—and this, I think, was the point the member raised, Mr. Chair—this in her recommendations: That Google delete the Canadian payload data it collected, to the extent that Google is allowed to do so under Canadian and U.S. law. If the Canadian payload data cannot immediately be deleted, the data needs to be properly safeguarded and access thereto is to be restricted.

What we're doing is precisely what the Privacy Commissioner asked, which is undertaking an analysis of both Canadian and U.S. law in terms of the laws of evidence and other applicable laws, to determine the extent to which it can be deleted. In the interim. we're doing precisely what she asked, which is maintaining the safeguards around the data and the protections for it.

Mr. Bill Siksay: Mr. Glick, what are those other applicable U.S. laws that are operative in this sort of situation?

Mr. Jacob Glick: It would be inappropriate for me to speculate on that, because I'm not a U.S. lawyer.

Mr. Bill Siksay: Are you—

Mr. Jacob Glick: But there's no mystery. In fairness, I don't want to leave you thinking that there's some mystery law here that hasn't been identified. It's precisely what the commissioner said in paragraph 69, which is simply the “applicable laws...including laws of evidence”.

Mr. Chair, members of this committee will be aware that there are, for example, pending lawsuits in the United States related to this issue, so we need to ensure that the laws of evidence are respected. It's not to say that any decisions have been made one way or the other. As I said in my opening, I think everyone here wants the exact same outcome, which is the deletion of all this data.

If I can say on a personal note—

● (1610)

Mr. Bill Siksay: Thank you. Sorry, but I'd like to ask Dr. Whitten a question.

Dr. Whitten, can you tell us which countries where Google collected payload data have seen that payload data deleted at this point?

Dr. Alma Whitten: I don't have the full list available in front of me, I regret. I know we have deleted it in several countries. Ireland, I believe, is one of the ones where we were able to quickly and simply delete it right away.

Mr. Bill Siksay: In the situations where it was deleted right away, are those countries where the data was held within that country's borders and not held offshore someplace? Has that affected the ability of Google to delete the information quickly?

Dr. Alma Whitten: I don't believe that has been an issue, but I would like to direct some of that question back to Mr. Glick, as I'm an engineer and not a lawyer, and that's a legal question.

Mr. Bill Siksay: All right. Given the Ireland example, do you know if the information was held in Ireland or was held offshore, outside of Ireland?

Mr. Jacob Glick: My understanding is that all the data was held in the same place, in fact, so this is—

Mr. Bill Siksay: So in that case, Mr. Glick, if all the data has been held in the United States and it has been deleted for some countries, wouldn't Google have already done the analysis about the applicable U.S. laws?

Mr. Jacob Glick: Well, don't forget that the Irish data was deleted on the advice of the Irish data privacy commissioner in May, or around May I should say, as I don't know the precise date. We weren't asked to hold on to the data for any period, and that can affect the analysis as well, because none of these class action lawsuits, for example, were in process at that time. I'm not a U.S. lawyer, so it's really irresponsible of me to speculate on—

Mr. Bill Siksay: You are Google's Canadian lawyer, though, aren't you, in terms of this issue? You are working on the analysis of the Canadian data for Google, are you not?

Mr. Jacob Glick: I'm Google's Canada policy counsel. In that role, I work on public policy issues relevant to Google here in Canada. Google is receiving other Canadian legal advice. To be clear, I'm not the person who advises Google specifically on the legal ramifications of what to do in Canada, although I am consulted on it.

The Chair: We're now going to go to Mr. Poilievre, for seven minutes.

Mr. Pierre Poilievre (Nepean—Carleton, CPC): Mr. Chair, before I begin, may I raise a point of order to clarify? Mr. Glick has raised the issue of his comments and the importance of prudence and making comments due to potential legal proceedings that could occur. I think he mentioned a potential class action lawsuit.

Can you clarify that nothing said here can be used in another tribunal and make precision for the fact that even though Mr. Glick and Dr. Whitten are not physically here, their comments are considered to have been made here in the context of a parliamentary organization, and therefore are given the standard parliamentary immunity?

The Chair: Just let me just double-check something.

Just on that point, I can give you my understanding of parliamentary law, and of course when you get into these international situations, it does become somewhat complicated. But Mr. Poilievre accurately stated that anything that's said before a parliamentary committee, including this committee, is subject to parliamentary privilege and, as a result, cannot be used in any courts, tribunals, or evidence-gathering bodies in Canada. What the Chair is not totally clear on—and I'm not going to opine on it—is whether that parliamentary privilege, which is well known, extends to other international bodies, like the U.S. Supreme Court. I don't have a definitive answer.

I don't know that answer, but I can tell you assuredly that anything said here—and that would include anyone who is testifying before the committee via teleconference—cannot be used in any other court, or tribunal, or body, for that matter.

● (1615)

Mr. Pierre Poilievre: In Canada.

The Chair: In Canada, yes.

Mr. Pierre Poilievre: And we don't have an answer as to whether or not it would be admissible in foreign tribunals.

The Chair: I wouldn't be in a position to give you an opinion on that.

Mr. Pierre Poilievre: All right.

If I could, I'll begin my questioning with the witness being aware of that ambiguity.

Mr. Glick, thank you for returning to our committee. On the question of the data elimination, you've indicated that data mistakenly acquired within the boundaries of Ireland has been deleted. Did I understand you correctly?

Mr. Jacob Glick: That's my understanding.

Mr. Pierre Poilievre: That was due to interactions that Google had with the Irish privacy commissioner?

Mr. Jacob Glick: Again, that's my understanding of the facts, yes.

Mr. Pierre Poilievre: And the reason that the data mistakenly acquired in Canada has not been deleted is because of ongoing discussions with the Canadian authorities on how best to proceed with that deletion. Is that correct?

Mr. Jacob Glick: Thank you for that question.

To clarify what I said, when I called the Privacy Commissioner in May to advise her of this unfortunate circumstance, I asked her what she wanted done with the data then. She asked that we preserve the data because perhaps she wanted to launch an investigation or review it in some manner. In fact, her office did launch an investigation and did review the data. We held on to the data at that time.

At the same time, conversations like this were happening in other places in the world. A level of analysis was done at that time in those other places. Where it was deemed appropriate by the local data privacy authority, and where it was deemed appropriate under the various legal systems, data was deleted.

We are now *x* number of months down the road, and we need to do that analysis given the circumstances of today, not the circumstances of May.

Mr. Pierre Poilievre: Perhaps I missed something, but did you say that some of the Canadian data has been deleted?

Mr. Jacob Glick: No, I didn't say that.

Mr. Pierre Poilievre: I may have misheard you. The data were originally retained, then, on the instruction of the Canadian Privacy Commissioner. Is that your testimony?

Mr. Jacob Glick: Yes.

Mr. Pierre Poilievre: Have you received any subsequent instructions to the contrary?

Mr. Jacob Glick: We received the Privacy Commissioner's interim letter of finding, which the committee has in its possession, and which she released to the press and to the committee in October. It asked that we delete the data as soon as we had assured ourselves that we are able to do so under Canadian and U.S. law.

Mr. Pierre Poilievre: You are in the process of securing those assurances through an analysis of the aforementioned laws?

● (1620)

Mr. Jacob Glick: That's correct.

Mr. Pierre Poilievre: Feel free to refrain from answering this if it requires unwarranted speculation: is there anything in either nation's statutes that might cause you to hold onto the data for an extended period of time?

Mr. Jacob Glick: I wouldn't want to speculate on that. Ultimately, our objective is to delete all the data. We didn't want it in the first place, and we don't want it now, but we don't want to delete it prematurely and cause more headaches.

Mr. Pierre Poilievre: I don't want to taint any legal proceedings that may materialize through class action suits, but with respect to the possibility of litigation from people whose information was inadvertently acquired by Google, could the data in your possession be required as part of an evaluation of what data existed and what damages were incurred?

Mr. Jacob Glick: I won't speculate on the outcome of any particular litigation.

I can tell you that it's something we would object to producing in a court proceeding, precisely to protect the privacy of the people whose data were mistakenly collected. There would be an irony to class action litigants demanding the production of data that they allege contains private data, but I can't speculate on what tactics any person, litigant, or regulatory authority might take.

The point is that we would certainly object to the production of any of this in court, I can tell you that.

Mr. Pierre Poilievre: All right. Thank you very much.

I think my time has expired.

The Chair: Pretty well, Mr. Poilievre. Thank you.

We're now going to start the second round of five minutes each.

Dr. Bennett, you have five minutes.

Hon. Carolyn Bennett (St. Paul's, Lib.): Thanks very much.

I'm still a little bit concerned about the actual process for making sure this never happens again. I was a bit surprised to learn that the engineer who made this assumption about whether it was a significant privacy breach is still employed by Google.

As we try to push responsibility for making decisions in organizations down as far as we possibly can, I'd like you to outline what special privacy training will actually look like. Will the offending engineer be the person delivering this as some sort of equivalent to community service? I don't understand how this person can excuse what they did. I don't understand why they're actually still working for Google.

In every sort of training I've ever done, whether it was with family practice residents or new candidates, the basics are: know what you know, know what you don't know, and know to whom and when to go for help. If people are making this gross kind of assumption about what is or isn't a privacy problem, I'd like to know what kind of curriculum you're going to deliver. What does "intense training" mean when somebody at that level has been able to pull off this rather massive breach with whatever previous training there was?

● (1625)

Dr. Alma Whitten: Thank you. That's an excellent question. I'm very glad to have a chance to answer it in more detail.

What the member said about making sure that you know what you don't know and that you know who to ask is very key to the training and the process improvements we're putting in place. It's very important for us to educate all of our engineers and product managers, but we're not going to be able to make them international experts in all aspects of privacy. If we were to aim to do that, it would not be setting up to succeed.

Above all, we want to educate them to not try to figure this out for themselves. Privacy is a complex topic, and addressing it properly within Google—or anywhere, really—requires a wide variety of expertise. It requires expertise in law, obviously and most certainly. It requires technical expertise to make sure there's a clear understanding of what exactly the technology is doing, what the systems are doing, and what the potential of that technology is. It requires expertise in the psychology of user understanding: of how the people who are going to interact with products will understand the options available to them. And it requires expertise in policy and communications in all of these things.

A very important point we will be making over and over again in our training is that individual engineers should never be making these judgment calls by themselves. We want to educate them on the privacy landscape and privacy concerns.

We want to very much educate them on Google's own articulated privacy principles of transparency, control, and responsible stewardship above all, but we also want to educate them very, very strongly and reinforce that education in many ways on the improved processes we are putting in place, to make sure that those fail-safes are there, that the thoughtful review is in place, and that individual engineers don't try to "lawyer" questions by themselves.

Hon. Carolyn Bennett: How much time would a newly hired engineer be given in privacy training now? What are you doing in service for the people who are already working for you? Would there be scenario planning and problem-based learning, which are usually viewed as modern ways of going about this?

Dr. Alma Whitten: For newly hired engineers, we expect to give them a significant session of privacy training within their first two weeks at the company, before they would be writing any code, before they would be starting on any product development. With that initial training, we expect to lay a lot of the seeds in place in putting the framework in place for them to know who they are supposed to talk to and when, to know where the resources are internally to help them understand privacy and to understand our privacy processes, and where those are quickly and easily found—all of those aspects of who they should talk to.

For engineers going forward, for the people who aren't going to be hired next week or the week after that to come in through this initial training, we will be doing follow-up training. But above all, I think, the process, which we are enhancing and optimizing now, and the training have to really be two halves of the same coin that will reinforce each other and work closely together.

The process will force engineers to engage with the training at various parts of their project's life cycle. As they are expected to engage with the process, then the training is there to tell them how to do so and to provide them help to enable them to do so. The goal is very, very much for those two aspects to strongly reinforce each other to make this as effective as possible.

The Chair: Thank you, Dr. Bennett.

Ms. Davidson, you have five minutes.

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

Thanks to our witnesses here today, both by video conference and in person. This is an issue that we're all taking very seriously, and certainly we have a lot of questions about it still.

My first question is for Mr. Glick, please. It's in regard to the letter we received, which the chair read out. I'll simply read the clause that I'm not clear about: “With respect to your question regarding any impediments under U.S. law to the deletion of the Canadian data, Google is working on analyzing the information and Jacob will give the committee an update on Thursday”.

What I would like an explanation of is “working on analyzing the information”. I don't know what you mean by “analyzing”, and when you're referring to “information”, are you referring to the data?

● (1630)

Mr. Jacob Glick: Thank you for asking for that clarification. No, we are not talking about analyzing the data. Google has no interest in trolling through the data, as we've said from the beginning, so thank you for allowing me the opportunity to clarify.

I think this is just a poorly worded sentence, and you should take it at face value, which is that we're doing the analysis that the Privacy Commissioner and our own due diligence require of us, which is to ensure that we're in a legal position to be able to delete the data, as I've described to a number of members of the committee.

Mrs. Patricia Davidson: Thank you very much, Mr. Glick. I appreciate that information.

I'd now like to ask Mr. Ramsay a question.

How many employees do you have in your group?

Mr. François Ramsay: Do you mean all of the company?

Mrs. Patricia Davidson: Yes.

Mr. François Ramsay: We have approximately 4,000 employees.

Mrs. Patricia Davidson: Okay. What do you do for privacy training? Do you have a privacy officer or somebody in a comparable role? Is privacy training done? If you do have it, could you outline that training?

Mr. François Ramsay: As I've outlined before, I am the privacy officer of the company. As such, I assume the responsibility of that office. In hearing the responses provided by Mrs. Whitten, I made good note of the point that we should be training our employees on privacy issues. Actually, I'm going to bring that to the office and see how we can address it.

Mrs. Patricia Davidson: So right now there is no privacy training as such.

Mr. François Ramsay: There's no specific privacy training going on at Yellow Pages.

Mrs. Patricia Davidson: Talking a little bit about Street View, can you tell me how widespread that is in Canada? What's the main target audience? Will it be expanded? If it will be expanded, how do you go about notifying people? Are you required to notify people for expansion?

Mr. François Ramsay: Maybe I'll simply tell you that MapJack, which is the initial service that we rolled out back in 2009 through Canpages, only covers the commercial areas of the cities of Vancouver, Toronto and Montreal. As far as the rest of the country is concerned and outside of these areas, maybe Martin can—

Mr. Martin Aubut: In the other cities, we use Google Street View. That is the second service we tested where we didn't have MapJack.

Mrs. Patricia Davidson: How many areas is Google Street View present in right now?

Mr. Martin Aubut: It's in the cities where MapJack is not. By default, let's say, Quebec will be Google Street View.

Mrs. Patricia Davidson: So it's Edmonton, Ottawa, and London, Ontario...?

Mr. Martin Aubut: Voila. Yes.

Mrs. Patricia Davidson: It's in all of those places. Is it in smaller areas as well or just in larger cities? Is it in the city of Sarnia, which is in my riding? Is it in rural areas?

Mr. Martin Aubut: For now, it's more in the major cities.

Mrs. Patricia Davidson: Is there a population size that you base it on?

Mr. Martin Aubut: No. In the beginning, this was a marketing play, so MapJack was launched in the core big cities, where there is a lot of population. We didn't have a strategy to go to other types of cities. The strategy was for the major cities.

Mrs. Patricia Davidson: What are the plans to increase the penetration?

Mr. François Ramsay: Generally speaking, I think our plan is that we would provide this service to the extent that we can obtain it from Google or Microsoft.

● (1635)

Mrs. Patricia Davidson: So you would purchase the finished product?

Mr. François Ramsay: Actually, my understanding is that this service is made available by Google to websites such as the Yellow Pages, or where information about merchants is provided.

Mrs. Patricia Davidson: So there wouldn't be another camera vehicle or whatever going up and down the streets?

Mr. François Ramsay: We are not in the business of mapping and collecting that information. We would buy it from a third party if it was for sale, or license it from a third party.

Mrs. Patricia Davidson: Would it be from a third party that already has it? Your third party collector in Hong Kong, a small company, must have come out and done the area you requested. They would not have had that information.

Mr. François Ramsay: The answer is yes. In the future, we would rather use services such as those offered by Google or Microsoft. They are firms that people are familiar with.

The Chair: Thank you, Ms. Davidson.

[*Translation*]

Mr. Laframboise, you have five minutes.

Mr. Mario Laframboise (Argenteuil—Papineau—Mirabel, BQ): Thank you very much.

Mr. Glick, my question is for you. A little earlier, you perhaps misunderstood my colleague's question. I am going to read you a report in a *Daily Mail* article from last Friday:

> "After having admitted "accidentally" gathering much more than information on Wi-Fi networks with its Street View cars last month, Google has just agreed to erase the private information gathered in Great Britain," Christopher Graham, the UK Information Commissioner, announced today. "I applaud the fact that the data captured from Wi-Fi networks can finally be destroyed," he said.

This means that, in Great Britain, Google agreed to destroy the data it collected. If I understand you correctly, you have not done so in Canada because the Privacy Commissioner asked you to keep the data. Is that correct?

[*English*]

Mr. Jacob Glick: Well, let me take a step back. First of all, I understand that we have agreed with the report from the Privacy Commissioner's equivalent in the United Kingdom, who has accepted our desire to delete the data in the U.K. I don't know that we've actually deleted the data yet. That's the question that's open in my mind and I just don't know the answer to that.

But the same is true in the Canadian context, which is that we also want to, desire to, delete the data in the Canada context. The only question is whether we are allowed to under the law and we have to do the analysis to determine whether we can or not.

What I was saying earlier with respect to the Privacy Commissioner was that initially, in May, when I contacted her office, she asked that we retain the data so that they could review it as part of an investigation, which they did undertake and which they did complete. Now, having concluded that investigation, they are saying that we are free to delete the data. We accept that, and we want to delete it, but we have to conduct the proper legal due diligence.

[*Translation*]

Mr. Mario Laframboise: You say that you want to check whether the law allows it. Which law are you talking about, Canadian law or American law? Your data are kept in the United States, if I am not mistaken.

[*English*]

Mr. Jacob Glick: Again, we're doing the analysis just as the Privacy Commissioner envisioned it in her report, which is that U.S. and Canadian law are applicable here—potentially.

[*Translation*]

Mr. Mario Laframboise: My next question is for Mr. Aubut. You understand how complex the Google case is. A little earlier, you said that you do not know the technology that your subcontractor uses.

What guarantees do you have that he is complying with the law, with Canadian law, if you have no control over the technology? How can you reassure us, Mr. Aubut?

Mr. Martin Aubut: I can tell you that we have specifically asked MapJack, the third party, if they gathered any other information. They told us that they did not, because it was not their basic task. That was to take pictures.

We do not believe that they have the technology to gather data. Anyway, I have to wonder why they would, I cannot give you an ironclad guarantee that they—

● (1640)

Mr. Mario Laframboise: You do not know, because, as you said earlier, you are not familiar with their technology.

Mr. Martin Aubut: We know one thing at the moment. I am familiar with images and image gathering. The service we provide to our users is the images. I cannot tell you about other information that MapJack may have gathered in the same way as Google.

Mr. Mario Laframboise: That does not reassure us. You are not aware of the information you are transmitting and you are not aware of the technology that was used.

Mr. Martin Aubut: I know the technology that we use for our service. For us, MapJack is not about looking for information. MapJack lets you see a specific address, because you can see a picture of it. That is all we use it for.

Mr. Mario Laframboise: But MapJack still works for you. You gave them a contract to get images for you.

Mr. Martin Aubut: They give us images, and that's it.

Mr. Mario Laframboise: You give them the work. If they contravene the Access to Information Act when they capture the images, you know that you are also legally responsible.

Mr. Ramsay, you are a lawyer, I understand. Are you aware that you are responsible because you employed a subcontractor who could use the data for which you signed a contract?

Mr. François Ramsay: We are aware of that, of course. Just this morning, I asked one of Martin's colleagues to tell me a little about MapJack's technology and to compare it with Google's. He told me today that the technology was much less sophisticated, much less specialized than Google's or Microsoft's.

It is actually a "no frills" technology. That is perhaps an appropriate term to describe the kind of product that MapJack has developed. We got permission to use MapJack's technological know-how, if I may put it like that.

You are right. Like any of Yellow Pages Group's suppliers, they do things with us. We trust them when we have no reason to believe that they are telling us anything but the truth. Very sincerely, we have been very clear about the matter. We really did not believe that there had already been a problem like this. It was never brought to our attention when we were dealing with MapJack.

However, given the committee's work and given the questions that Google has been asked, we were proactive and we asked MapJack to provide us with the confirmation. They did so with no hesitation.

The Chair: Your time is up, Mr. Laframboise.

[*English*]

Mr. Albrecht, you have five minutes.

Mr. Harold Albrecht (Kitchener—Conestoga, CPC): Thank you, Mr. Chair.

I want to thank our guests for being here today and also our online guests for joining us.

I think it's important to take a step back and remember what got us into this study in the first place. It was the concern relating to Street View and the collection of images. But I think from my understanding of where we are at this point, we agree that it's a very useful tool and a worthwhile project. The privacy concerns that were initially at the forefront I think have largely been addressed, with the blurring of faces and licence plates and also the rapid removal of images upon the request of the users. I'm happy about that part.

As it relates to inadvertent data collection, I think all of us still have some concerns that this issue shouldn't have arisen, but I think Google has handled it in a very responsible way. We have legitimate concerns around this table, and I think all Canadians are concerned about the protection of their private information, but Google has, as I've said, taken positive steps to correct the mistake that was made. I, for one, appreciate that.

You've apologized for the error. You're taking concrete steps to ensure that this sort of situation doesn't reoccur. Also, as I understand it, you're working in close partnership with the Privacy Commissioner to be sure that you are in fact in compliance with Canadian law.

My question is to Dr. Whitten. It relates to the international aspect of privacy. Does Google have a privacy expert for each country? Or do the efforts of the privacy commissioners from the various countries, as they meet in their international conferences and work out some types of agreements across international boundaries, help you enough to create a level playing field so that there's not a need for an expert for each and every country?

● (1645)

Dr. Alma Whitten: Thank you for that question.

I would say it is really a combination of both. We do have local expertise on the ground in as many countries as possible—in fact, in most countries. I spoke to the earlier question from the member about the need to bring in all of these different kinds of expertise across legal and engineering functions.

We're also very conscious of that cross-culturally, and of the need for our privacy review to bring in perspectives from all of the different parts of the world where our products are going to be seen, used, and experienced. That's part of the reason why I am now based in Europe: to make sure that even in my own person I can bring in a little bit of extra balancing, having started out in the United States and then bringing that over there.

Canada is certainly one of the countries where we pay very, very close attention to the work of your Privacy Commissioner and to her voice on the international stage. We rely very heavily on Jacob's relationship and close communications with her office. We do similar things in all of the countries where we're present.

Mr. Harold Albrecht: Thank you for the response to that question.

Just to follow up with a very brief question, do you find that as the international privacy commissioners get together and discuss these issues, it is helpful for you as the overall director of Google's privacy concerns?

Dr. Alma Whitten: Very, very much so, and thank you for returning to that point. For us as an international company operating on a global scale, it's certainly tremendously helpful when the world state-of-protection authorities come together and attempt to work out a consensus on how to approach these matters. Because, of course, if we can do the right thing across all of our products and all of our services globally and have it be the same right thing, that obviously is tremendously helpful to innovation and also to our users.

Mr. Harold Albrecht: I do think that the proactive approach of preventing problems before they occur is certainly very worthwhile.

If I have another minute, I'd just like to ask Mr. Ramsay a question.

You indicated earlier that at this point you don't have specific privacy training. Do you, though, have any connection or regular contact with the Privacy Commissioner in terms of consulting with her and in terms of moving ahead with addressing the privacy concerns that affect us?

Mr. François Ramsay: Historically, we've not had these relationships. I have to tell you, though, that I've determined with some of my colleagues that this is something we'd be interested in exploring and being proactive about. We understand that as the world becomes more digital, obviously, many of these issues will come to the forefront. It's important for us to be on top of these matters and to be responsive and proactive on legitimate privacy concerns that Canadian institutions have.

Mr. Harold Albrecht: Okay. But to this point you don't have direct contact with the Privacy Commissioner?

Mr. François Ramsay: No.

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

Mr. Siksay, you have five minutes.

Mr. Bill Siksay: Thank you, Chair.

I want to come back to Dr. Whitten. I want to ask, just so I'm clear that the collection of Wi-Fi access points wasn't intrinsic to the collection of street-level images, whether I am correct that it wasn't something that was necessary to the whole process of building Google Street View in that sense.

Dr. Alma Whitten: That's correct.

Mr. Bill Siksay: Has Google looked at the whole question of the privacy implications of collecting Wi-Fi access points? I know that we've discussed the payload data question and discussed the collection of street-level images, but this is specifically about the privacy implications of collecting Wi-Fi access points. Is this something that Google has investigated or considered?

Dr. Alma Whitten: Yes, and there are a number of points I would make in response to that.

The first is that in the collection of basic Wi-Fi access point data in order to provide a geolocation service, which I will explain a little more in a moment, we were not being particularly innovative. We were latecomers to that field.

I'm aware of a number of companies in the United States, in Germany, and around the world that were already doing this: collecting the basic Wi-Fi access point information in order to provide geolocation services. In looking at this, we probably looked around and saw that this was already a standard in the industry and that in collecting the basic information we were not doing something new or different.

Just to provide clarity for what this information is and what the purpose of collecting it was for us, the simplest example I can give is to say that when you're standing on that street corner or you're in that taxi cab and you pull out your smartphone or your BlackBerry, it gives you a display of the wireless networks that it can see so that you can connect to them if they're open or if you're a subscriber to them. Exactly that information that your BlackBerry is seeing is what we would see and intend to collect. It's the information that is broadcast by every Wi-Fi service in order to allow people legitimately to see it and to connect to it.

The purpose of collecting this information is so that when I'm standing on that street corner and I want to use Google Maps, say, to give me directions to my destination, my cellphone, as part of that location service, can use the fact that it can see three different particular Wi-Fi networks, let's say, from where I am standing, as a way to detect my location in order to give me directions.

The reason for doing this in addition to or instead of the original traditional model using GPS—geographical positioning services—to provide the information is that, first of all, receiving that information from a satellite, as is done in GPS, is a much stronger power draw on the device that one is using, and it also doesn't work very well inside buildings. So the use of that basic broadcast information from Wi-Fi services to triangulate and to allow people's location to be determined to provide them direction is something that works very well. That's why quite a few companies have been doing it.

● (1650)

Mr. Bill Siksay: Thank you. That's a helpful explanation.

I don't know if you know that when the representatives of the Office of the Privacy Commissioner of Canada were last before the committee, their info technology research analyst, Dr. Andrew Patrick, raised a concern about the privacy implications of the collection of Wi-Fi access points. He said he would need to be reassured. I'll read for you what he said:

> There is a potential for concern. If information about the presence of a Wi-Fi access point can be at all linked to a particular individual, either individually or in combination with other bits of information, then it would be potentially personal information and therefore potentially something that we would be worried about.

Is that something that Google has considered particularly in the collection of Wi-Fi access points and has that kind of personal information—

Dr. Alma Whitten: Yes. The way in which—

Mr. Bill Siksay: Go ahead.

Dr. Alma Whitten: The way in which we collect that information does not link it to any personal information. Take me, for example, as a Google user with a Google account. The fact that Google drove by my house and mapped my Wi-Fi has no association with that. There is no data to link those two things together; they are completely independent.

Mr. Bill Siksay: Is this something that Google has checked since this whole issue came to the attention of privacy commissioners and users of Google?

Dr. Alma Whitten: We'll be continuing to check for such matters on an ongoing basis.

Mr. Bill Siksay: Do you know of any European country or privacy commissioner or related office in Europe that is investigating that issue or has launched an investigation into the privacy implications of collecting Wi-Fi access point data?

Dr. Alma Whitten: I am not aware of any investigations on that point specifically.

● (1655)

Mr. Bill Siksay: So you haven't been asked to participate or provide information to any...?

The Chair: Mr. Siksay, your time is up. We're going to move on. Thank you very much.

Mr. Easter, you have five minutes.

Hon. Wayne Easter: I won't take five minutes, Mr. Chair.

I'm a bit intrigued by what has happened in Ireland. I've been led to believe by the answers given that the privacy infringement of information collected in Ireland.... That data has been destroyed at the request of the privacy commissioner. That is correct, right?

Mr. Jacob Glick: Yes, but I want to clarify this. The destruction, as I understand it, happened at the time that we notified data privacy commissioners globally, so it happened in the late spring.

Hon. Wayne Easter: That's fine, Mr. Glick.

So the Irish privacy commissioner ordered the data destroyed, and it has now been destroyed. The Canadian Privacy Commissioner ordered the data destroyed, but it hasn't been destroyed.

Mr. Jacob Glick: The Canadian Privacy Commissioner said that the data should be destroyed presuming that we don't have any legal obligations to otherwise preserve it.

Hon. Wayne Easter: Run that answer by me again.

Mr. Jacob Glick: The Privacy Commissioner of Canada, in her letter of findings, said that the data should be destroyed to the extent that there aren't any other legal obligations to preserve the data. She was clear about this in her report. Actually, my recollection is that when she testified before this committee, her evidence was that there might be reasons beyond the control of her or of Google that would require the data to be retained, and that an analysis has to be done to ensure that the other obligations we would have are met.

When the data in Ireland was destroyed, an analysis was done, and we concluded that it was okay to destroy that data. The same analysis is happening today for the Canadian payload data. It's just that the analysis is happening at different points in time, and therefore there are different facts on the ground, because things changed between now and May—mainly, all sorts of investigations and legal proceedings that may make it more complicated to destroy the data. But again, I'm not an expert in the rules around that, so I can't opine on those considerations.

Hon. Wayne Easter: I guess what I find difficult is why it was destroyed in one area, but in the other area it isn't. It has the same implications on privacy whether it's in Ireland or in Canada, I would expect. Where was the Irish data stored? Was it in the U.S. as well? I understand that there could be some U.S. implications, maybe, but where was the Irish data stored?

Mr. Jacob Glick: In my understanding—and if I'm wrong, I'll report back to the committee via letter—all the data was stored in approximately the same place in the United States. So the data that would have been destroyed relevant to Ireland was stored in the United States before it was destroyed, but again, it was destroyed at a different point in time, and therefore the analysis that was done had different factors to consider, so....

And you have my answer on that, I guess.

Hon. Wayne Easter: Okay. I'll leave it at that. I'll ponder that for a while. Thank you.

The Chair: Thank you, Mr. Easter.

Mr. Siksay, you have five minutes.

Mr. Bill Siksay: Thank you, Chair.

Mr. Glick, who at Google could explain to us which U.S. laws are in play in terms of the analysis that needs to be done regarding the destruction of the Canadian data held in the United States?

Mr. Jacob Glick: I don't know specifically who that would be. I'd have to consult internally.

Mr. Bill Siksay: Could you do that and let us know who at Google would be the person who could answer those kinds of questions for us?

Mr. Jacob Glick: I can do that, but I should say that if the committee is interested in learning more about analysis of U.S. law, there will be all sorts of.... There are a lot of complications and moving parts to this. It might make sense, if the committee continues to be interested in this, to give us the chance to actually undertake the analysis and to conclude what we can and can't do. We can write to the committee at that time, when we write to the Privacy Commissioner to advise her of the conclusions of the analysis—

● (1700)

Mr. Bill Siksay: Thank you, Mr. Glick.

But I do suspect that Google has done some of that analysis already if they've already moved to destroy data held from some countries as opposed to others, if all the data was held in the United States. I do hear your point on that, but I am interested in finding out who at Google could explain which U.S. laws are in play here.

I have another question about the specific technology that Google deployed in the cars. I understand that a particular program developed by the engineer at Google is responsible for collecting the payload data. I just wanted to know if Google sold, leased, or lent to any other company or agency—or anyone else—this particular program, so that someone else might have used this in the same way that Google did and didn't know they were collecting the payload data. Was anyone else using this particular program?

Dr. Alma Whitten: To the best of my knowledge—and I would be surprised if my knowledge is not correct—this code was entirely inside Google and was never shared.

Mr. Bill Siksay: Okay.

I wanted to ask another question. This is going back to the street-imaging question. I know that when we first addressed the street-imaging question, Google did undertake to destroy the unblurred images that Google felt it was necessary to keep for a year, I believe. I'm just going from memory here, so maybe I should be corrected. I also understood that they would hold those images outside of Canada as well, but that they would be destroyed after a year. Have any of those images been destroyed at this point?

I guess I should have asked the first question: when did Google first start the street-imaging process in Canada? Has that deadline of a year passed in the collection of any of those street images and has that led to the destruction of the unblurred images?

Mr. Jacob Glick: Sir, I can report back that what we said was we would “bake in the blur” one year after the publication of the imagery, and as far as I understand it, we've done that successfully.

Mr. Bill Siksay: So you've baked in the blur, but what about the original images that were collected, the unblurred ones. Have they been destroyed?

Mr. Jacob Glick: Sorry. That's.... To be clear, yes.

Mr. Bill Siksay: Is that through that process of baking in?

Mr. Jacob Glick: As far as I understand it, that's the case.

Mr. Bill Siksay: So it's through that process of baking in, so there isn't a separate data bank of unblurred and blurred images?

Mr. Jacob Glick: No. “Baking in” is a term of art; I think maybe I invented it. I'll claim credit in any event, even if I didn't. So for a year there would be, as you say, two corpuses of data, the public data to which the blur is applied, and the data held internally. At the end of a year, post-publication, there is no longer any data that has unblurred imagery in it. The same data that Google has is the imagery that's public, which is including the blur. I understand that's been done for the Canadian imagery.

Mr. Bill Siksay: Chair, I just had one request for information from our witnesses from Google. I wonder if it would be possible to get a list of countries in which payload data was collected and an indication of where and when it was destroyed, and also where that data was stored for each particular country, so that we know, for instance, if it was collected in a country where it was stored and whether it's been destroyed at this point.

The Chair: Have you heard that?

Mr. Jacob Glick: I did hear it, Mr. Chair, and I'd be happy to undertake to answer the member's question in writing.

I should say, thought, that the process we've gone through here in Canada is being played out in other countries of the world, and as investigations conclude in those countries and a similar analysis is undertaken, the answer may change. So whatever I tell you will be for a specific point in time, but it may be that afterwards we'd delete some data. But yes, the answer is that I will provide in writing to the committee, to the best of our knowledge, the answers to those questions.

● (1705)

The Chair: Mr. Glick, could we ask for that information within two weeks?

Mr. Jacob Glick: I think that should be fine. If there's a problem with that, I'll let you know.

The Chair: Thank you very much.

Mr. Jacob Glick: If a problem arises, give me till the seventeenth.

The Chair: Thank you, Mr. Siksay.

Mr. Bill Siksay: Could I ask two more quick questions, Mr. Chair? I hope they're quick. I don't know if you have other people on your list.

The Chair: Perhaps I'll come back to you, Mr. Siksay.

I just have an issue that we have to get addressed, Mr. Ramsay. This is on the whole issue of your launch of Canada Eye. There was a press release from your company in March. According to my reading of it, you're combining information taken from the iPhone 3GS compass, GPS systems, and video cameras simultaneously to determine information on where a person is. Then you can identify nearby businesses and how people can get there in real time, which would include the direction and distance.

This kind of follows up on some of the issues that Dr. Bennett was raising. Do you feel that all of these systems working simultaneously meet with the Canadian privacy legislation policies?

Mr. François Ramsay: The answer, to the best of my knowledge, is yes. Specifically on smartphones, for instance, the service we're using to provide directions for people is, again, with services that are provided by the likes of Google and Microsoft.

The Chair: But do you get the location of the individual using their own video cameras on them, that you have access to, and their GPS system?

Mr. François Ramsay: I'm sorry. I don't understand.

The Chair: On the Canada Eye system, if I were walking down the street and I used it, would it have my location by using video cameras and a GPS system?

Mr. François Ramsay: I'm not sure what Canada Eye refers to.

The Chair: I'm going from the analyst's notes and your own press release. I'll just quote it.

Mr. François Ramsay: Which press release is this?

The Chair: On March 10, 2010, Canpages launched “a free augmented reality” iPhone application. The quote reads:

> The Canpages application enables users search for a specific business category—from local delis and mom and pop bakeries to Starbucks and Tim Hortons—and then shows the direction and distance to all of the businesses in the category in the local area. Essentially, CanadaEye is one application to find everything nearby as well as how to get there in real time.

It also states:

> Augmented reality is the latest technology coined for applications that leverage the iPhone 3GS' compass, GPS and video camera simultaneously.

Now, don't ask me to explain all of that.

Voices: Oh, oh!

Mr. François Ramsay: No, no. That's fine. I'm sorry. This additional context is extremely helpful. Thank you for that.

I don't know if some of the members here have iPhones, but there is a button on the Canpages application that you can use. I'm more familiar with another one from a competitor of Canpages, YPG. Basically, you use the camera feature of your iPhone, pointing in a direction, and listings are pushed using the GPS features of the iPhone or the smartphone that you're using. Basically, all that it's doing.... The image is a bit of a gimmick, I guess, in the sense that it's not really the eye that is seeing. It's just that the iPhone understands in which direction it is pointing and therefore understands which businesses are located in the direction in which you are pointing.

So just to confirm, it's not strictly speaking the fact that the camera sees a business that it identifies it. It's just that it's geocoded. The businesses are geocoded, and the phones pointing in that direction push the listing that is being provided.

The Chair: Thank you very much. It's all very clear now. The fog has lifted.

Voices: Oh, oh!

The Chair: Madame Thi Lac, you have up to five minutes.

● (1710)

[*Translation*]

Mrs. Ève-Mary Thaï Thi Lac: Good afternoon, Mr. Glick. I would like to get more information about some of the things you said a little earlier. When my colleague Mr. Laframboise asked about Canadian and American law, you said that there were legal obligations. So I would like to know which takes precedence when you go to do your checking.

Will it be American law or Canadian law when you compare the two? Does one contradict the other? If American law is less precise than Canadian law, which one will take precedence?

[*English*]

Mr. Jacob Glick: I think it would be irresponsible of me to speculate before the analysis is complete.

[*Translation*]

Mrs. Ève-Mary Thaï Thi Lac: Who checks those obligations? Is it the commissioner or Google?

[*English*]

Mr. Jacob Glick: Who checks on which...? Sorry?

[*Translation*]

Mrs. Ève-Mary Thaï Thi Lac: When you talked about checking, you said that you had to check your legal obligations. Who does the checking, the commissioner or Google?

[*English*]

Mr. Jacob Glick: It's our own internal analysis.

[*Translation*]

Mrs. Ève-Mary Thaï Thi Lac: A little earlier, you told us that you chose to store the Google Street data in the United States rather than in Canada.

[*English*]

Mr. Jacob Glick: I think it's because we were convinced that having the data in one place was the best way to ensure that it was safe and secure. That was important to us. It was also important, I should add, to the Privacy Commissioner. She mentioned in her report that it was important for the data to be safe and secure and for Google to have stored it in a safe and secure manner.

[*Translation*]

Mrs. Ève-Mary Thaï Thi Lac: Are all the data that you have gathered in different countries stored in the same place?

[*English*]

Mr. Jacob Glick: As far as I understand it, that's the case. I should add.... We covered this last time, but I'll just give you a bit of perspective in terms of the amount of data for Canada.

My understanding is that, roughly speaking, it's the amount that could be stored on a USB thumb drive that you could purchase at Best Buy for about $50 in terms of the total quantum of data. The total quantum of data globally that was collected and that we're talking about here would fit on a hard drive that you could purchase for about $120 at Costco.

[*Translation*]

Mrs. Ève-Mary Thaï Thi Lac: Thank you, Mr. Glick

My next question goes to Mr. Aubut. You said that you could not give precise information about the technology used by your subcontractor.

Is it possible to provide that information to the committee in the next few weeks?

Mr. Martin Aubut: Certainly.

Mrs. Ève-Mary Thaï Thi Lac: Good. Thank you.

[*English*]

The Chair: Mr. Siksay.

Mr. Bill Siksay: Thank you, Chair.

Mr. Glick, can you tell us if, as a result of the collection of the payload data, Google has faced criminal charges, administrative penalties, or sanctions anywhere around the world?

Mr. Jacob Glick: I don't have a running scorecard. I don't mean to be flip, but I'm not familiar with all of the proceedings that have happened globally with respect to this.

I can tell you that globally there have been, as I said before, investigations by data privacy authorities throughout the world, and various of these have different levels of authority. Also, various governments have taken different levels of interest, and I just don't know the outcome of every single one of those cases.

Mr. Bill Siksay: Dr. Whitten, would you have the answer to that question?

Dr. Alma Whitten: No. As I've said, my focus has been on the internal improvements inside Google. It has been our legal and policy teams that have been handling the interactions with data protection authorities in each country.

● (1715)

Mr. Bill Siksay: Mr. Glick, is that something you could track down for us and provide to the committee as well?

Mr. Jacob Glick: Could you say that again so that I understand precisely what I'm agreeing to?

Mr. Bill Siksay: I want to know if Google has been subject to criminal charges or administrative penalities or some other kind of sanction anywhere as a result of the download of payload data.

Mr. Jacob Glick: To be clear, you're not asking for a list of the outcomes from every data privacy authority, but rather about whether we've been subject to criminal penalities in other countries of the world.

Mr. Bill Siksay: They could be administrative penalities. I'm sure that not every privacy commissioner issues a criminal charge or goes to a criminal charge. But could you tell us if there were administrative penalties of some kind?

Mr. Jacob Glick: I'll do my best to try to get you an exhaustive list of those outcomes.

Mr. Bill Siksay: Thank you.

Chair, I have to add again,that I'm a big fan of Google and a user of Google. I couldn't run my daily life without Google. I have really serious questions about this, because it is such an important service to all of us. I want to make sure that this kind of thing doesn't happen in the future and that all of us who depend on Google in a very big way can use it in the knowledge that our privacy is protected.

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

Colleagues, that concludes the questions. I'm going to ask all the witnesses if they have any closing comments or remarks to make to the committee.

I'll start with Mr. Ramsay.

Mr. François Ramsay: Thank you for having us.

We hope we've answered your questions. If there are any further questions, we'd be happy to appear in front of the committee again.

The Chair: Do you have anything, Mr. Aubut?

Mr. Glick, is there anything you want to leave with the committee?

Mr. Jacob Glick: I want to thank the committee again for turning its attention to this matter. It's obviously a very serious matter, one that we are taking incredibly seriously to ensure that something like this never happens again and that we continue to earn the trust—which the member just spoke about—of our users every single day. We're committed to that.

The Chair: Dr. Whitten, is there anything you want to leave with the committee?

Dr. Alma Whitten: I would add to Mr. Glick's my thanks for the committee's questions, feedback, and interest in this matter. I feel very strongly that we share the goal of making sure that nothing damages the trust of our users and that everyone's data is safe with us.

The Chair: There's one minor matter that I want the committee to deal with.

At this point in time, I want to thank all four witnesses for appearing here today. I think the meeting was very instructive and very interesting.

I also want to especially thank the people who were involved in the House of Commons technology. We've had two witnesses here via video conference, from two continents, using two languages, and I think everything went very smoothly. Thank you for that effort.

Witnesses, you're excused.

Perhaps we'll suspend for two minutes and then come back.

● _____ (Pause) _____

●

The Chair: I call the meeting back to order.

The only other matter I want to deal with is to follow up on Mr. Calandra's motion. I don't think it's necessary to read it again. When we left last meeting, there was a motion tabled with the understanding that Monsieur Ménard would be invited to attend, and then I would bring it back to this meeting.

That invitation has been extended. The information we have is that he has absolutely no problem coming before the committee, but for different reasons he would prefer to come via a motion passed by the committee. I'm just going to ask the clerk if that is a correct summation.

● (1720)

Mr. Jacques Maziade (Clerk of the Committee, Standing Committee on Access to Information, Privacy and Ethics): Absolutely.

The Chair: Okay. Such being the case, I would urge the committee to bring back the motion that was tabled. We said that we would. It's back before the committee right now. You have the motion moved by Mr. Calandra.

Is there any discussion?

(Motion agreed to [See *Minutes of Proceedings*])

The Chair: Okay. I understand that he will be appearing on Thursday, December 2, for one hour.

There being no further business, the meeting is adjourned.

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