House of Commons
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 028 • 3rd SESSION • 40th PARLIAMENT

EVIDENCE

Thursday, October 28, 2010

Chair

The Honourable Shawn Murphy

Standing Committee on Access to Information, Privacy and Ethics

Thursday, October 28, 2010

● (1530)

[*English*]

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

This meeting, colleagues, is a regular meeting of the Standing Committee on Access to Information, Privacy and Ethics. It's a continuation of our study on street imaging applications, in particular dealing with the situation concerning Google, Canpages, etc.

We were hoping to have officials from the Office of the Privacy Commissioner of Canada and officials from Google and Canpages here at the same time, but that didn't work out. The Google people are coming next Thursday. We will have Mr. Jacob Glick with us for the first hour next Thursday, November 4.

However, we're very pleased to have with us today, to deal with this particular issue, three officials from the Office of the Privacy Commissioner of Canada. The committee would like to welcome first Patricia Kosseim, general counsel. She's accompanied by Daniel Caron, legal counsel, legal services, policy and parliamentary affairs branch; and Andrew Patrick, information technology research analyst.

I believe Madame Kosseim will give the opening remarks for the office. I will now invite her to give her opening remarks.

Again, welcome.

Ms. Patricia Kosseim (General Counsel, Office of the Privacy Commissioner of Canada): Thank you very much. It's indeed a privilege to be here. We thank you for inviting us to appear before you as you conclude, I believe, your study on street-level imaging technology. We're here to assist you in any way we can.

I'm Patricia Kosseim, general counsel. As the chair already indicated, with me are Dan Caron and Dr. Andrew Patrick, from our IT advisory services. On behalf of the Privacy Commissioner, I would like to relay her regrets at not being able to be here in person, as she is currently out of the country.

I'm going to give a brief overview of some recent developments that have occurred in this area since you last heard from former assistant commissioner Elizabeth Denham, who appeared before this committee in October 2009.

[*Translation*]

Prior to Google Street View being launched in Canada last year on October 7, 2009, the Office of the Privacy Commissioner of Canada, along with our provincial counterparts from British Columbia, Alberta and Quebec, issued a Fact Sheet on street-level imaging entitled "Captured on Camera: street-level imaging technology, the Internet and you". The purpose of that sheet was to offer Canadians more information on the privacy implications of street-level imaging technologies.

We outlined our views to businesses rolling out such technologies. We asked them to take the following steps.

They had to be proactive and creative to ensure that Canadians know when they may be photographed.

These businesses should also employ proven and effective blurring technologies for faces and vehicle licence places.

Third, they must offer fast and responsible mechanisms to allow any images to be blocked or taken down upon request.

Lastly, they must have a good reason to keep original, unblurred images and they must also protect them with appropriate security measures.

Since our last appearance before this committee in October 2009, the Office of the Privacy Commissioner of Canada has continued to stress the importance of ensuring that privacy remains an utmost consideration in the development of new products and services. However, events of the last year show that organizations need to build greater personal information protections into their new products while they are being developed. The incident involving Google's collection of Wi-Fi payload data from its street-level imaging vehicles is an important lesson in that regard.

● (1535)

[*English*]

In May 2010, Google discovered that in an effort to collect information about Wi-Fi access points to enhance its location-based services, its Street View cars had inadvertently been collecting payload data from unsecured wireless networks. Essentially, payload data is information about the communications that run through these networks. Google promptly grounded its Street View cars, stopped the collection of Wi-Fi network data, and segregated and stored by country all of the data already collected.

Pursuant to the Personal Information and Protection of Electronic Documents Act—PIPEDA—as you know well, the commissioner may initiate a complaint in respect of an organization's personal information management practices if she believes there are reasonable grounds to investigate the matter. On June 1, 2010, our office sent a letter to Google stating that the commissioner in this case and as per her statutory discretion found reasonable grounds to investigate and had initiated three complaints against the company.

The complaints initiated by the commissioner were: first, that Google's collection, use, or disclosure of payload data was done without the prior knowledge and consent of the individuals affected; second, that Google's collection of payload data was done without prior identification of the purposes for which they were collecting this data; and third, that Google's collection of payload data was not limited to that which was necessary for the purposes identified.

In the course of our investigation, representatives from our office, including Dr. Patrick, went to the Google Mountain View facility on July 19, 2010, to review samples of the payload data collected by Google. Following the investigation, which included several exchanges between our office and Google, the commissioner issued her preliminary letter of findings on October 19, 2010.

As the commissioner stated in her recent appearance before you on October 19, her investigation found that Google had inappropriately collected personal information of Canadians from unsecured wireless networks. In some cases, that personal information was highly sensitive, including complete emails, user names and passwords, and even medical conditions of specified individuals. Unfortunately, this collection of data was due to an error that could have been easily avoided if Google's own procedures had been followed.

Essentially what happened here was that the engineer who developed the code to sample categories of publicly broadcast Wi-Fi data also included code allowing for the collection of payload data, thinking that this type of information might be useful to Google in the future. The engineer had identified what he believed to be "superficial" privacy concerns, but contrary to company procedure failed to bring these concerns forward to product counsel, whose responsibility at Google would have been to address and resolve these concerns prior to product development.

The investigation revealed that a number of privacy protection principles under PIPEDA had been violated, and accordingly, in her preliminary letter of findings, the commissioner recommended that Google re-examine and improve the privacy training it provides to all its employees, with the goal of increasing staff awareness and understanding of Google's obligations under privacy laws. She also recommended that Google ensure it has an overarching governance model in place that includes effective controls to ensure that all the necessary procedures to protect privacy have been duly followed prior to the launch of any product, as well as clearly designated and identified individuals actively involved in the process and ultimately accountable for compliance with Google's obligations under privacy laws. Finally, she recommended that Google delete the Canadian payload data it collected, to the extent that it is allowed to do so under Canadian and U.S. law. If the Canadian payload data cannot immediately be deleted for legal or other reasons, the data must be properly safeguarded, and access to it should be restricted.

At this time, the commissioner considers the matter to be still unresolved. The matter will be considered resolved only upon receiving, either by or before February 1, 2011, confirmation from the company that it has implemented the above recommendations, at which point the commissioner will then issue her final report and conclusions accordingly.

● (1540)

We look forward to Google's implementation of our recommendations and hope that they will from now on ensure both in procedure and in practice that effective measures for protecting personal information are built into their new technologies at the very early stages of product conception and development. Our office will continue to ensure that the protection of privacy remains a key consideration for organizations prior to launching the products or services, so that Canadians may benefit from creative and innovative products secure in the knowledge that their personal information is being protected and that their rights as consumers are fundamentally respected.

Thank you.

The Chair: Thank you, Madame Kosseim.

We're now going to start the first round. That's seven minutes each. We're going to start with Madam Fry, seven minutes.

Hon. Hedy Fry (Vancouver Centre, Lib.): Thank you very much. I understand what you've said, and I understand that you're waiting until January. In the meantime, am I understanding that Google has denied any doing of this intentionally? It was all sorry, we made a mistake, people weren't properly trained, etc.

In the meantime, do you feel comfortable that you can accept Google's word that they are going to comply at least with the intent if not with all of the things they said they would do? And there is a real concern that employees at Google, if they have access to this information, could personally use it in instances when they know some of the people and could go out there and either psychologically or whatever, blackmail, use this against a person they happen to know in personal conversations. Are you satisfied that this isn't happening? That's my first question.

Secondly, you know that in Europe they have taken far more stringent steps than I think the Privacy Commissioner is suggesting to Google here, which is kind of that Google get its act together, do what it's supposed to do. In Italy and in Europe, they don't seem to think so. What they're asking is that Google vans have stickers saying that they are collecting payload data and that they notify the communities through which they're going, three days before they go there, both in terms of some kind of communiqué, posters, or whatever, and on radio and in newspapers, so that people can shut down some of the things that they're doing at the same time. Because this is a real invasion of privacy. This could be serious in many instances. It could lead to all kinds of complications for people, not only in terms of embarrassment, but in terms of theft. People will know a lot of things about when people are home, where they're going for holidays, and could therefore know that their homes are ready for rifling. There could also be situations in which a person is having a simple conversation that is misinterpreted by someone to be criminal activity when it isn't.

So I think this is a huge issue and I would like to have your answer on these two questions. One, are you satisfied? Do you trust Google at this point in time? And, two,what about the European regulations?

Ms. Patricia Kosseim: Thank you for that question.

Mr. Chair, I will address it in three subparts.

The first was a question as to whether or not we are confident that Google will be implementing the recommendations. We have not received any official response from Google. We have read the newspapers, as all of you have, in terms of the statements they have made to the press indicating that they have already undertaken major steps to remedy the problem, but we await Google's official response.

The reason the commissioner issued a preliminary letter of findings is that she doesn't want just undertakings: before concluding the matter and determining whether it is fully resolved or not, she wants proof and evidence that the recommendations have actually been implemented. She is waiting for actual implementation, and not just undertakings. That's the first question.

The second question was on whether we're worried about the data that has been improperly collected. I believe that in the course of the investigation, that was one of the elements that was investigated. The security measures that Google has taken to protect and segregate the data that were improperly collected have been found to be adequate. They have secured the data. They have limited the number of copies. They have secured the information in a secure location, and I think the investigation concluded at that point that it is sufficiently safeguarded pending and awaiting its ultimate destruction.

The third question was on more stringent actions being taken in Europe. I'll answer with respect to two things. The first is in respect of the improper collection of Wi-Fi data, which is the outstanding issue right now.

All data protection commissioners around the world, as you know, have different powers. Some have powers to impose and levy fines or impose criminal sanctions. They all have different powers. In terms of the different reactions, in large measure I would say they're not reflective of interpreting the situation at different levels of severity, but that they vary because of the different powers commissioners have under their respective jurisdictions.

Our commissioner has exercised all of her powers under PIPEDA in order to complete the investigation and in order to bring Google, through her ombudsman role, to implement its recommendations before she concludes the matter and further explores other avenues available to her under the act.

Those are my comments in terms of different reactions in Europe and elsewhere around the world to the Google Wi-Fi matter and the improper collection of payload data.

In respect of its street-level imaging technology and the deployment of that technology generally, I'd say there has been more coalescence and harmony around accepted practices. You're absolutely right to indicate that our best practices, issued in conjunction with our provincial counterparts, indicate that one best practice for the deployment of this technology is to notify neighbourhoods before you come through with your Google cars or any other cars. That notification can either be by way of a public means of announcement or by having cars properly labelled, etc. There are best practices that have been recommended and followed.

● (1545)

Hon. Hedy Fry: Thank you.

I think it was indicated that I have one more minute.

Do you believe that the commissioner's power with regard to certain sanctions, whether fines or criminal sanctions, is the same as it is for commissioners in Europe? Is it less than in Europe?

Ms. Patricia Kosseim: Well, it varies. Even in Europe, it varies from one jurisdiction to another. Her powers under PIPEDA do vary from those of commissioners who have powers to impose fines, for instance.

The model under PIPEDA has worked well to date. She has used all the powers available to her in this case and in others, and hopefully there will be a productive conclusion. Her powers—

Hon. Hedy Fry: Is her power less than that found in many European jurisdictions?

Ms. Patricia Kosseim: It is less than in some other jurisdictions, yes.

The Chair: Thank you very much, Madam Fry.

Go ahead, Madam Freeman, for seven minutes.

[*Translation*]

Mrs. Carole Freeman (Châteauguay—Saint-Constant, BQ): I want to thank you for being here today, Ms. Kosseim, Mr. Caron and Mr. Patrick.

I'd like to talk about Google. I find it somewhat hard to accept what is going on with this international business. It's everywhere, it sets up everywhere, and I must say it acts somewhat cavalierly. I think that it's completely crazy to say that this was a mistake. When you have Google's powers, technology and structure, if you are a socially responsible business, you ensure that training is provided and that it is serious. Google gathers information on people's private lives in such a way... In fact, my personal information and yours are becoming products in the market.

This multinational is establishing itself in all countries. One commissioner protects personal information in Germany, another does the same thing in Australia, and there is one in Canada and another in Quebec. Can't you agree to try to standardize the requests made to Google? It seems to me that it's currently David vs. Goliath. Every time you make a move, Google develops a new technology, and there may be a mistake. That's my first question.

I would like to put the second to Mr. Patrick. Did he go with Ms. Stoddart to visit Google this summer? Did he make the trip?

● (1550)

Ms. Patricia Kosseim: Yes.

Mrs. Carole Freeman: I would have liked to know how that went and what he saw. What new technologies can we expect from Google or other companies that, once again, might not respect people's privacy? Can someone answer?

Ms. Patricia Kosseim: I'll answer the first question, with your permission, Mr. Chairman, and then I'll ask my colleague to answer the member's second question.

First, was it crazy to say there was a mistake? Yes. Should that mistake have been prevented? Yes. Had Google adopted procedures to ensure such a mistake would not occur? Yes. Were the procedures followed? No, and that's where the commissioner reacted more strongly, for Wi-Fi, as in the case of Google Buzz and Google Street View. The commissioner's key message was that, when these new technologies are developed, the procedures to ensure protection must be put in place and followed from the product design and development stage, not just when an error occurs. That's the key message. These measures must be immediately followed and there must be control mechanisms to ensure they are followed in every case.

Would it be preferable to harmonize reactions to the various technologies developed by Google? That is the wish of many commissioners around the world who have powers in the privacy field. They increasingly want to work together to face large global businesses like Google. Now, the possibility of doing so varies from one commissioner to the next since they don't all have the same powers regarding the exchange of information with their counterparts elsewhere in the world.

Consequently, with regard to Bill C-28 before you, the Fighting Internet and Wireless Spam Act, it would make a key amendment to the Personal Information Protection and Electronic Documents Act that would enable our commissioner to freely exchange the information that she receives in the context of her investigations with her counterparts elsewhere in the world so as to be able to react in a more concerted and harmonized manner and deal with large businesses such as Google.

With your permission, I'll ask Dr. Patrick to answer your next question.

[*English*]

Dr. Andrew Patrick (Information Technology Research Analyst, Office of the Privacy Commissioner of Canada): Thank you for the question.

Commissioner Stoddart was not in attendance with me in California. It was myself and Dr. Whalen, who's also a technical analyst. What we saw there was what is described in the report and the statement that we've read. We saw examples—and we only looked for examples—of personal e-mails, personal communications, names, addresses, web traffic being requested and replied to, chat messages, those kinds of things. Our strategy was simply to get an idea of the extent of the data, the nature of the data, to see examples of personal information and then to stop. That's exactly what we did.

[*Translation*]

Mrs. Carole Freeman: What kind of welcome did you get? Did you have access to everything you wanted?

[*English*]

Dr. Andrew Patrick: Yes, we did. We got a very good reception. We were able to witness how the data was being stored, how it was being encrypted. We got full technical support, which is what we were looking for. We were there to do a technical analysis. We got full support. We were given instructions on how the data is stored in Google's proprietary formats, how it can be read, how to search. We got very good cooperation.

[*Translation*]

Mrs. Carole Freeman: From what you could see, what new technologies can we expect from Google? They aren't just created overnight.

[*English*]

Dr. Andrew Patrick: It doesn't happen overnight. We know that there are a number of areas in which Google and many other companies are working. There's a real emphasis on personalized services, various kinds of services, services that you will carry in your pocket. So these are location-based services that will know where you are, what your interests are, and will provide recommendations. This is a big area where many companies are working.

We also know, for example, that Google is moving into the entertainment business and is launching a home television service. Again, this will have the possibility of being personalized towards your viewing habits and your desires. Both of those have potential for having privacy implications since both of those are things that we're carefully monitoring.

● (1555)

[*Translation*]

Mrs. Carole Freeman: Geolocation is already underway. It's possible to find people and that's already a problem.

Could you describe for us the potential privacy threats that the other technologies you've just described pose?

[*English*]

Dr. Andrew Patrick: Thank you.

There's a variety of different dangers. There are obviously personal safety dangers. If people are able to use location technologies in order to track someone's physical whereabouts and they want to do that person harm, if the data is not properly controlled, then there's that danger. There's also an issue of more expanded commercial services, commercial use of the data. An example of this is whether the data about where you are could be used for more and more advertising.

The Chair: Merci, Madame Freeman.

We're now going to move to Mr. Siksay, seven minutes.

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

Ms. Kosseim, Canpages also used similar technology, also had a process to do a similar thing in terms of street-level imaging. Do we know if they collected payload data as well in the course of doing their photography for their application?

Ms. Patricia Kosseim: No, we have no knowledge of any such collection nor of any intention to collect Wi-Fi radio signals or payload data. We have no knowledge of that.

Mr. Bill Siksay: In your introduction today and in comments from folks, from the commissioner and others, it seems like what we thought Google was doing was a photographic process that was linked to some kind of cartographic process. Your description today of what we thought they were up seems to all pertain to photography. Did we know before May, when the Germans discovered the Wi-Fi, that they were looking for Wi-Fi access points? Did we know that was part of what they were doing before May 2010, or was the commissioner under the impression that it was a photographic process?

Ms. Patricia Kosseim: Mr. Chair, we received, as did all data protection authorities, notice from Google in April 2010 that they had intended to collect and were collecting publicly broadcast Wi-Fi radio signals. This was with a view to enhancing its location-based services in order to pick up and to identify the availability of radio signals in the neighbouring area and the relative distance to their automobiles.

As a question of practicality, they were proceeding to collect that data at the same time they were collecting street-level photography, because they had the cars going around anyway. So they announced that they were putting antennae on the roofs of the cars to at the same time collect and capture the neighbouring Wi-Fi radio signals.

What Google did not say, because Google did not know until May, prompted by requests for further information from the German data protection authorities.... They realized in May and publicly announced in May that unbeknownst to them as an organization, they were also collecting not only the radio signals and the presence of those signals, but communications and the content of communications being picked up and travelling through those signals, if I may say. This we found out in May of 2010.

● (1600)

Mr. Bill Siksay: You're saying that in April 2010 they notified you that they were doing this extra piece. But they had launched the service back in October 2009. So had they been collecting that information prior to April 2010, or was that when they began doing it? Were they just confirming that they had been doing that all along and that it had been part of the photographic work they had done prior to that?

Ms. Patricia Kosseim: What they began to do earlier was street-level photography, which they announced they were deploying in Canada. What they announced in April 2010 was the addition of antennae on their automobiles, with a view—I believe prospectively—to also collecting Wi-Fi radio signals.

Mr. Bill Siksay: So it seems that they weren't doing this initially, when they began to do the photographic work to launch their service; that they hadn't initially been collecting data on Wi-Fi access points.

Ms. Patricia Kosseim: My understanding is that when they deployed the product initially and announced they were deploying the product in Canada, as they had in the U.S., it was with a view to street-level photography imaging—

Mr. Bill Siksay: Only?

Ms. Patricia Kosseim: Yes, initially.

And by their correspondence to data protection authorities in April 2010 they announced this now-added feature that they would be doing by placing antennae on the roofs of these cars to prospectively also pick up and publicly broadcast Wi-Fi signals.

Now, I have no knowledge of how early they did that, other than the date at which they notified that they would be doing it.

Mr. Bill Siksay: Okay.

Is there any intrinsic connection between doing the photographic street images and collecting the Wi-Fi access points? Is that necessarily linked? Do you have to collect the Wi-Fi access points to be able to use the street imaging technology appropriately?

Ms. Patricia Kosseim: No. My understanding, Mr. Chair, is that the street-view imaging technology collects the photographic images of your neighbourhoods that you all see on your Google maps when you Google your neighbourhood, as I'm sure you have—as I have. That is a product in and of itself.

This new enhancement is an additional idea developed by one of their engineers, to include in the code at the same time not only images, but also to pick up radio Wi-Fi signals. And this afterthought, or this additional enhancement, was with a view to improving their location-based services.

If you would like an explanation of the business rationale for this enhancement, I could ask my colleague to explain how that actually enhances location-based services.

Mr. Bill Siksay: I would appreciate knowing that, yes.

I take it that's you, Dr. Patrick.

Dr. Andrew Patrick: Yes, it is.

When you have a device such as a cellphone or a BlackBerry, it has often built into it the ability to help you locate yourself. Most modern devices now can use three technologies simultaneously: GPS, if you can see the GPS satellites; the cellphone tower information from whatever cellphone towers it's able to see; and also this Wi-Fi data. When you walk into a strange street you can determine what satellites are visible, but also whether there's a Wi-Fi from a local coffee shop, or from the Joneses next door, and that information can be used to recognize where you are.

Mr. Bill Siksay: I'm still struggling with when we knew they were using Wi-Fi data. It sounds as though it can be used as an enhancement of the street imaging process, but it wasn't necessary for it. It improved as it went along, or something like that. Is that possible?

Dr. Andrew Patrick: In their statement to us and to all the data protection authorities in April, they said basically that they were taking advantage of the fact that they were driving the cars around anyway,—

Mr. Bill Siksay: Okay—

Dr. Andrew Patrick: —but it really is a separate technology and a separate service.

Mr. Bill Siksay: Okay.

Is there any privacy concern about the collection of Wi-Fi access points? I know there's clearly a concern with payload data, but what about collecting data about Wi-Fi access points? You talked about their being a public broadcast, and unprotected, and you said people haven't taken steps to protect their wireless networks, but it is there a privacy concern specifically about collecting data about Wi-Fi access points?

● (1605)

The Chair: Thank you, Mr. Siksay.

Ms. Patricia Kosseim: May I ask Dr. Patrick to address that question as well?

The Chair: Yes, please.

Dr. Andrew Patrick: 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.

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

We're now going to move to Ms. Bennett. Ms. Bennett, you have seven minutes.

A voice: Do you mean Mrs. Davidson?

The Chair: I'm sorry; it's Mrs. Davidson.

We'll go to Mrs. Davidson for for seven minutes, and then we'll go to Ms. Bennett.

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

Thanks very much for being here with us this afternoon.

As you can tell, we've got a lot of questions. I think we're almost to the point—at least I know I am at the frustration level—where the "Oops, sorry" scenario is getting to be a little bit thin. We need some firm assurances. We need to know what direction we're taking. The speed and the diversity of our development of technology today make it imperative that we have some better things in place to regulate it and to show we are secure.

Going back to what Dr. Fry asked about the unsecured sensitive information that was inadvertently collected, whether it was inadvertent or whether it wasn't is immaterial at this point; how do we know that there weren't violations when it was collected? Do we know for sure that the information was not used for something it shouldn't have been? Do we have a way to know that?

Ms. Patricia Kosseim: Mr. Chair, the announcement that Google made when they identified the "oops", as you say, was a public announcement in May of 2010, announcing to the world that they had inadvertently collected payload data. They immediately halted their automobiles and immediately halted further collection of Wi-Fi data.

In the course of our investigation, to my knowledge there was no indication to lead us to suspect that anything untoward had been done with the data that had been inadvertently collected. As soon as it was identified, as I said earlier, the investigators were confident that appropriate security measures had immediately kicked in and segregated and secured the data appropriately.

We have no knowledge or any reason to believe, from the basis of the investigation, that anything untoward was done with the data that were collected.

Mrs. Patricia Davidson: Okay.

We've also heard this afternoon about some new technologies that Google is exploring at this point. Could you talk a little more about those technologies? I've read a little bit about this issue, and what I have read is not reassuring unless we are able to put some restrictions or some regulations in place. Could one of you please speak a bit to those new technologies that they're anticipating?

Ms. Patricia Kosseim: I'll give a few general remarks and then I'll ask my colleague to elaborate.

In the introduction of any technology and in other areas of science—and in the case of information technology increasingly so—we've generally taken measures to adopt what is commonly known as the precautionary principle. As you introduce and deploy new technologies, in the absence of scientific evidence indicating with absolute certainty that there are no harms being done, the precautionary principle kicks in. It says that you must take the proactive measures—the "forecare" measures, to use the German term—to avoid risk. You must take those measures necessary to avert the potential harm that may arise. This is the key message that the commissioner and her colleagues worldwide are sending to organizations, especially those that, like Google, are model organizations and trendsetters: to adopt the spirit of the precautionary principle before deploying new information technologies.

I'll ask Dr. Patrick to speak to you about the specifics of this new technology.

● (1610)

Dr. Andrew Patrick: Thank you for the question. I'm hoping it's something you'll ask Google next week.

We don't have any special knowledge of the kinds of things they're developing. We watch the trade press and attend the technical conferences. We know the kinds of things that they and other companies are exploring. Location-based advertising is going to be a big trend; sending advertisements to your mobile phone or your home entertainment system, based on where you are and what your profiles are, are things that we're well aware of, and we're watching for them. Beyond those specifics, I don't have any special knowledge.

Mrs. Patricia Davidson: Thank you.

Am I correct that the commissioner is at an international conference right now?

Ms. Patricia Kosseim: Yes.

Mrs. Patricia Davidson: Do you expect that she'll be bringing back recommendations, best practices, improvements, or things we can discuss at this committee on an international basis?

Ms. Patricia Kosseim: Yes.

Every year at this international data protection commissioners' conference, data protection authorities from around the world, including the FTC in the U.S., come together and typically prepare and adopt resolutions as a community. There will be resolutions coming out of this international meeting. I'm sure the commissioner would be pleased to come back and speak to this committee about the 2010 resolutions that will have been adopted by her and her counterparts to tackle some of these global issues. I'm sure she'd be pleased to do that.

Mrs. Patricia Davidson: Thank you.

Do I still have some time?

The Chair: You have 40 seconds.

Mrs. Patricia Davidson: The Wi-Fi issue is still unresolved, and you're waiting to hear something on it before February 1. Are you feeling fairly confident that you're going to get something, given the degree of cooperation? You have indicated there has not been a lack of cooperation. Are you confident that you're going to be getting what you need by that date?

Ms. Patricia Kosseim: I think we have every indication to be confident. Although there have not been formal responses to us from Google, we have heard responses in the press, as all of you have, to indicate concrete steps that they have already taken. In the course of our investigation we learned about steps that had already been undertaken to begin the process of putting in place appropriate governance structures within the organization, which is a global giant, as you can understand. The date of February 1 was deliberately chosen, bearing in mind a reasonable amount of time not only to make these changes but also to have concrete evidence that they've been made at a global scale. That's why that date was given.

We have every hope that we will get a positive response earlier than that, and we'd be delighted to do so. We are fairly confident that there will be a good ending to this.

The Chair: Thank you very much, Mrs. Davidson.

Can I ask you one question before we go to the second round, Madam Kosseim?

This is a hypothetical question. In your opinion, what would have happened in this situation if Google had not been caught by the Germans six months ago?

Ms. Patricia Kosseim: To my knowledge and to be fair, I don't think they were caught by the Germans. I think that prompted by questions, in essence they caught themselves, identified the breach, and announced it right away. I have no personal knowledge of it, but that's my understanding.

If it had not been identified when it was, I think the danger would have been in just complacently continuing, on the understanding or the thought that they were, in the engineer's terms, "superficial privacy concerns". The belief was that any data picked up would be so scrambled anyway by the speed at which the cars go by that it would be meaningless. It would not be meaningful data. I think the danger of not identifying it and stopping immediately would have been the continued complacency in not understanding the privacy implications, and of course the more you collect, the greater the risk to citizens' privacy.

Essentially those are the risks, and as we've seen in other instances, the more you collect, the more risk you have of something untoward happening to it. There is a greater risk that it will be leaked or otherwise breached. The risks just compound from there.

● (1615)

The Chair: Thank you very much.

We're now going to start round two.

We're going to go to Ms. Bennett. Ms. Bennett, you have five minutes.

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

My line of questioning, instead of following everybody else's, has to do with how we go forward.

At an international meeting, obviously people like the commissioner come together to consider what we do about this. Surely we have now learned something from this Google Street View episode. I was a bit shocked that just one engineer can decide that this is a "superficial" privacy concern and then go forward. It doesn't seem as though there's any training at all as to what privacy is. They're naming Alma Whitten as the new director of privacy; do we know who that person is, or whether she has any idea of privacy? Would the equivalent people in lots of other companies that are obviously pushing us forward in technology be at the privacy commissioners' meeting? Where do they find out what the minimum specifications actually are in terms of determining what a real privacy concern is, or a medium one, or a so-called superficial one? We're breaking new ground all the time, and I think that even in medicine we learned the hard way that the law has a terrible time keeping up with technology.

Do you have any observations as to what you would want us to put in a report from this committee about how we could go forward? Could it be that the commissioner needs powers more like those of some of her international counterparts? At the same time, the NHS is able to tell people where the closest smoking cessation course is, and that's probably a good thing, so how do we balance the need to help citizens get things that are relevant and responsive to their needs against their need for privacy?

I think this example was pretty egregious. Google all of a sudden was capturing all of this data without any pre-clearance or advance warning or respect. Somebody who knows more about privacy than a private enterprise would actually need to go forward the way we would, with a law and a charter challenge. We would want to know whether this would fly or not before you went ahead and collected all this stuff.

If you were writing the recommendations for this committee as to what we learned and how we can go forward in a more proactive way, what would those recommendations be? If you don't have them now, would you send them to the committee?

Ms. Patricia Kosseim: That's a very nice question. Thank you.

We may take you up on that on further reflection and send those recommendations back to you. I'm sure our office would be pleased to do so, but let me offer a few suggestions right off the bat, if I may.

The first thing I could say is to echo what has been the key message of the commissioner and her international counterparts, which is to impress upon all organizations—but especially model organizations and world trendsetters like Google—that they must take proactive measures to avert risks before the deployment of products and services occurs. This is a key message; if you were to echo it, I think it would be very helpful.

There are other things being contemplated by Parliament right now that would go a long way in assisting in where we go from here. One of those is to afford the commissioner with the powers and the authority necessary to share information about ongoing investigations with her international counterparts, so that she can compare notes with her German and U.K. and Irish and Australian colleagues and discuss what we have found, what they have found, and what we need to do collectively to stop something in its tracks.

Currently, she cannot do that, but Bill C-28 would afford her with the powers to share and exchange information and collaborate even more meaningfully than she can now with her international counterparts to deal with these global issues.

Another change going from here currently to Parliament would be to give her discretion to choose which complaints she goes forward with. Right now she must investigate all complaints, which takes an awful lot of resources, as you know. If she were afforded with the discretion to set priorities and decide where the real risks are, to take some complaints or not investigate other complaints, then she could afford and allocate resources much more meaningfully to get at the big risks—such as Google, in this example—and allocate her resources accordingly. That discretion would help.

Finally, another change before Parliament is Bill C-29, the amendments to PIPEDA. As you know, these amendments would make it mandatory for organizations to notify of breach. This would go a long way towards bringing these instances out into the open to be able to deal with them.

● (1620)

The Chair: Thank you very much.

Go ahead, Mr. Albrecht, for five minutes.

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

Thank you for being here today.

I wanted to follow up Bill C-28 and Bill C-29. I take it from your comments that you are very supportive of the measures in those bills that are before Parliament right now.

Ms. Patricia Kosseim: I know that the commissioner is on record as supporting particularly those provisions I just mentioned. I know that there are many things that she welcomes in the bill, and if asked to do so, I'm sure she would discuss in further detail her position on other issues.

Mr. Harold Albrecht: Thank you. I wasn't intending to ask the question, but you opened that door on Bill C-28 and Bill C-29.

I'd be the first to acknowledge that I'm not an IT expert, and my questions will probably show that quickly enough.

If Google can inadvertently capture this Wi-Fi payload data while a car is driving down the street, how can I be assured as a private citizen that some IT expert with malicious intent could not go down my street, do a personal investigation on my data, and use it for something other than proper purposes?

Ms. Patricia Kosseim: Mr. Chair, one of the key outcomes and messages coming out of this investigation is that although Google has a large responsibility, there is the other side of the coin, which is that individuals and organizations who use wireless networks have to adopt the protective measures necessary to encrypt data so that you, I, or anybody else going down the street cannot pick up information about their communications.

That is a big responsibility of individuals and of organizations as well.

Mr. Harold Albrecht: So it's unencrypted information from people who are carelessly leaving their Wi-Fi accessible to people in the apartment next door that's the big issue.

I want to follow up on a question that Ms. Fry asked about private information. She alluded to the possibility that you could even tell from the pictures that somebody was on holiday. I want to follow that up.

The information and pictures that are being gathered by Google Street View are not being gathered every day. It's once a year or once every six months or once a month. How frequently are they updating? Are the chances of telling whether I'm home pretty remote, or am I wrong on that?

Ms. Patricia Kosseim: My understanding is that these are still photographs taken at a point in time. They're snapshots at a point in time. They can capture other compromising information, but they are a snapshot in time.

Mr. Harold Albrecht: Okay. If I am a private citizen who is not surfing Google every day, and something private was posted on Google Street View, how would I be notified? How would I ever find out that there may have been an image there for six months that I didn't even know about? Is there any way of finding out that kind of information?

Ms. Patricia Kosseim: The first thing you can do, as a citizen, is to Google-map the area of your neighbourhood. That's for starters.

● (1625)

Mr. Harold Albrecht: That's assuming that you have a computer and that you're accessing Google and that you care whether you're on there or not before you find out there's a problem.

Ms. Patricia Kosseim: Yes, you're absolutely right.

It's not an obvious answer, but when you do identify a concern, our understanding is that the take-down measures are much better and much clearer. They are accessible and responsive in both Google and Canpages, as examples of the organizations we've been discussing. Those take-down measures can be exercised, and you can get a fairly responsive reaction.

Mr. Harold Albrecht: For the person who has a computer and is on Google, it's simply a matter of sending them a message, but for the person who isn't computer-literate at all, or who doesn't have one, is it a telephone call? Could you call to remove your information?

Ms. Patricia Kosseim: I'm not sure. I don't know of methods other than the computer procedure.

Mr. Harold Albrecht: I can ask that question next week.

Do I have some time left?

The Chair: You have about a minute, Mr. Albrecht.

Mr. Harold Albrecht: Okay.

Do we have any idea what percentage of the streets in Canada are currently on Google Street View? Is it 80%, or 50%, or are we closer to 100%?

Ms. Patricia Kosseim: I don't know. Maybe that's another one you could ask Google. I'm not sure.

Mr. Harold Albrecht: I think I will probably leave it at that.

Do I have 30 seconds?

The Chair: Sure, go ahead.

Mr. Harold Albrecht: Maybe I'll put a question to our legal counsel.

In your opening remarks, Ms. Kosseim, you mentioned on page 5 that one of the things you recommend is that "Google delete the Canadian payload data it collected, to the extent that Google is allowed to do so...".

Why would they not be allowed? In what circumstances would they not be allowed to remove data they've collected illegally in the first place? I was wondering if Mr. Caron would—

Ms. Patricia Kosseim: I think that you've asked this question of legal counsel.

Dan, would you respond?

Mr. Daniel Caron (Legal Counsel, Legal Services, Policy and Parliamentary Affairs Branch, Office of the Privacy Commissioner of Canada): Thank you for the question.

The recommendation was articulated in that manner because there are ongoing litigation matters in the United States. A number of civil actions have been commenced against Google with respect to this matter, and the commissioner wouldn't want to suggest that Google spoliate any evidence that might be relevant to those proceedings. That's the reason.

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

[*Translation*]

Ms. Thi Lac, you have five minutes.

Mrs. Ève-Mary Thaï Thi Lac (Saint-Hyacinthe—Bagot, BQ): Good afternoon, Ms. Kosseim, Mr. Patrick and Mr. Caron.

My question is further to that of my colleague Mr. Albrecht and concerns stored data. You talked about the procedure for removing images. What in general are the deadlines for the removal of those images?

Ms. Patricia Kosseim: First, I'd like to clarify one point. Faces and licence plates have been blurred for some time now. So we're not talking about that, but rather about other images that nevertheless constitute a concern for the individual in question.

I don't know exactly how much time that would take. I don't know whether we tested that, but I think so. I can't tell you the exact time it takes, but I believe the process is quite efficient.

Mrs. Ève-Mary Thaï Thi Lac: Yes, but you don't have any specific figures on the time it takes.

Ms. Patricia Kosseim: I'm going to ask Dr. Patrick; perhaps he knows.

[*English*]

Dr. Andrew Patrick: You should ask Google what their policy is or what their target is. Our experience is that it's happening within 24 hours.

[*Translation*]

Mrs. Ève-Mary Thaï Thi Lac: That's good.

Despite the fact that you talked about blurring licence plates and faces, I would like to know what is being done for the public interest. Consider the protection of certain women who are victims of spousal abuse. What happens if someone finds images of women's centres and homes, primary or secondary schools? Even though certain images are blurred, I nevertheless find it somewhat difficult to accept that.

The public interest and especially the protection of young children, minors and persons who are victims of violence are fundamentally important. What can be done to ensure the protection of these individuals by the Google Maps system?

Ms. Patricia Kosseim: I'm going to answer that question in two parts.

We know the practices of two companies, Google and Canpages. To give you an example, those two companies reacted to the same problem in very different ways. Google undertook to speak with certain vulnerable groups in advance to ask them what their preferences were and how to manage the problem. We know that it took the initiative of doing so and, to our knowledge, it did a good job of pursuing that approach.

In the case of Canpages, I believe the reverse was true. That company's policy is not to blur the images of buildings because that draws attention to the buildings that are not identified and that, for the reasons you mentioned, no one wants identified. I'm talking more specifically about buildings for women who are victims of violence, for example.

● (1630)

Mrs. Ève-Mary Thaï Thi Lac: I talked about women and children who are victims of violence. I understand that, when certain images are withdrawn, that further draws attention.

Could one policy be adopted for all educational institutions? That policy could concern minors, whether it be primary or secondary students. Will a policy be established for all these images to be removed?

Ms. Patricia Kosseim: As a best practice, we have recommended that the organizations use these technologies to begin a dialogue with neighbourhood organizations to determine how this problem can be managed as a whole. Our proposed best practice is that this conversation be held with the communities in question.

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

[*English*]

The Chair: Merci, Madame Thi Lac.

Mr. Shipley, you have five minutes.

Mr. Bev Shipley (Lambton—Kent—Middlesex, CPC): Thank you very much.

I'm not usually on this committee, so if some of my questions are not that relevant, that may be why.

Ms. Kosseim, I find this very disturbing. You seem to be, as part of the Office of the Privacy Commissioner of Canada, pretty subtle about it all. I don't know the back history. This company, from what I'm reading, has 23,000 employees. Technology is not something that is primary information to them. I'm reading here—and help me if I'm wrong—that Google said Friday that it aims to make sure that workers are obeying the rules. The company is also introducing tougher privacy measures, and they're going to make sure that their employees now understand what privacy means. I find that appalling.

It was just a few days ago in October that they said this, and it has been going on now for a year. This is a company that delves into people's privacy. They go down the street and take pictures of your place, pictures of your vehicles, pictures of who's in your yard, and all this stuff, and they're saying “Oh, we're going to blur this all out”.

The complaint part from June 1 mentions that Google's collection and use of data was done without the individual's prior knowledge. They actually hadn't thought, “Gee, you know, if we're going to be delving into somebody's private life, do you think maybe we should have actually thought about letting them know we're going to do it?” They said they did it without prior identification, so they never even thought about identifying people and talking to them.

The worst of it is that they were collecting data for which they had not identified the purpose. I know you said earlier that they didn't understand that. When they would be going down the street, it would be blurred or whatever the terminology was, and they didn't think. I think the biggest part is actually that they just didn't think.

I don't want to be cruel, but it would lead me to believe that this really would lead people to think about corruption. It really leads me to think that we've now got this huge multinational company that is intent on making dollars in some way. One of my colleagues mentioned that they're getting into the movie business, and they're running around the communities taking pictures of people's property without their knowing. They've been doing it for a while.

I have a question. How long were they doing this before they actually got caught? I know you said they didn't get caught, but actually they did. How long had they been doing it before somebody realized that the company was actually taking pictures of people's private lives and that perhaps they'd better stop, because now it was out? How long was that happening before the stoppage of it actually came about?

● (1635)

Ms. Patricia Kosseim: I have a couple answers.

Just to be clear, the commissioner was extremely concerned, so let me not understate that. The commissioner was extremely concerned, which is why she initiated this complaint right off the mark.

Mr. Bev Shipley: I didn't mean to take on the commissioner. I was just taking on the school board.

Ms. Patricia Kosseim: No, I just want to be clear and fair in my representation on her behalf.

She was first off the mark to initiate a complaint, has led a speedy investigation to get to the heart of the matter, and has in a precedent-setting way said, "I don't want just undertakings that you're going to do this. I want you to show me that this has been done before I will say and agree to say that it's been resolved." I think that's also important, to indicate the seriousness of the situation.

The other thing I just want to clarify is that we're talking about two different technologies or two different deployments. One is the taking of the pictures, which is something that had been going on much longer, and about which the commissioner wrote to the organization in 2007 to indicate that she had problems. So there has been a long conversation to get them to adapt their practices to comply with Canadian privacy laws. That's one.

Then the more recent innovation is the collection of radio Wi-Fi signals or publicly broadcast Wi-Fi signals. That is something very recent. As I said, I know only that on April 27 we received knowledge that they were doing this and that in May there was a problem. She responded on May 30.

Mr. Bev Shipley: I'm sorry, I missed that part of it. How long have they been doing the collection of the Wi-Fi signals? That's not just in Canada? Have they been doing it in the States?

Ms. Patricia Kosseim: My understanding is they've been collecting the Wi-Fi signals for about a year.

Mr. Bev Shipley: Do you know whether they knew they were picking up this personal information off these signals?

Ms. Patricia Kosseim: Our understanding is that they had no knowledge that they were picking up payload data, let alone personal data, which is what our investigation uncovered.

Mr. Bev Shipley: And you actually believe that?

Ms. Patricia Kosseim: That was in the investigation report. Part of the investigator's job is to assess credibility, and that was the outcome.

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

I have just one question arising from that last question and answer.

You say they didn't know they were picking it up, but all the evidence is that they were not only picking it up but storing it. They have actively stored it all, and it's 600 gigabytes. So how can we say they didn't know they were picking it up when they actually stored it?

Ms. Patricia Kosseim: I will repeat my understanding, and then I will ask Dr. Patrick to say it in better terms than I can.

There are two things. There are the publicly broadcast Wi-Fi signals that they knew they were picking up, and they intended to pick up. What they did not know was that in that collection, they were also picking up meaningful payload data, which means not only the signals themselves but the communications, contents of messages, that were being transmitted through those signals. That's the best way I can explain it.

Dr. Patrick.

Dr. Andrew Patrick: I'll just expand on that a little bit.

When we viewed the data, there was 18 gigabytes of it. That's about four DVDs' worth of data. That would have been intermixed with hundreds, or perhaps thousands, of gigabytes' worth of photographs collected at the same time. Google cars use a proprietary storage mechanism to compress all of the information they can onto as few hard discs as possible while they're driving around. All of this information is being heavily compressed and written to the hard drives within the cars, so it is possible that they just did not see that data there in among all the other data that was there.

The Chair: Thank you for that explanation.

Thank you, Mr. Shipley.

We'll now go back to Mr. Siksay for five minutes.

Mr. Bill Siksay: Thank you, Chair.

I think there are three pieces, as I am seeing them now. There's the photography piece about which we've raised questions and the commissioner has raised questions, there's the payload data piece, which I think we're waiting to hear back from Google on, and then there's the Wi-Fi access piece.

When I was last questioning you, Dr. Patrick, you said there are some privacy implications of collecting at Wi-Fi access points. Is there any investigation continuing about that at the present time to determine if there has been a violation of Canadians' privacy because of the collection of that particular data?

● (1640)

Dr. Andrew Patrick: Thank you for the question. It's a very good question. We have not been asked to investigate that particular aspect of data collection, so we've not looked into it in detail.

It was not part of this investigation, because we were looking specifically at the issue of capturing content. So what we have stated is what we know so far.

Mr. Bill Siksay: Do you know if anybody elsewhere in the world is looking at that particular aspect of this process?

Dr. Andrew Patrick: The Europeans have expressed concerns about the collection of the Wi-Fi access point information.

Mr. Bill Siksay: Okay. But we don't know if they've drawn any conclusion about that at this point?

Dr. Andrew Patrick: I don't remember off the top of my head. I think they're at a stage similar to ours of trying to make sense of it and trying to figure out what's appropriate.

Mr. Bill Siksay: Ms. Kosseim said at one point that Google sort of expected when they were driving down the street that any payload information they got would be so hopelessly scrambled it would be useless, and it turns out that wasn't the case.

I don't know if this is really an important question or not, but it just occurred to me. Does it mean that if the Google camera car stopped at an intersection, the people who lived around that intersection would be more at risk of having a direct transfer of their data because the car was stationary? And would that be true if they were on their lunch break and left it running or stopped at a traffic light, for instance?

Dr. Andrew Patrick: Thank you for the question.

Yes, if a car was stationary, more data would have been collected. The software in the cars was set to change channels. There are about 11 Wi-Fi channels. It was changing channels five times a second, so it wasn't like it was getting a continuous stream from the house it was parked across from, but it would get more and more samples of that information if the car was parked there.

Mr. Bill Siksay: And there'd be more likelihood of a complete sample of information being transferred in that kind of circumstance?

Dr. Andrew Patrick: Yes.

Mr. Bill Siksay: Okay.

Ms. Kosseim, can you tell us which officials of Google the commissioner's office deals with?

I gather we have Mr. Glick coming next week. Is he the person you deal with, or are there other people who are privacy specialists at Google you would deal with to answer your questions?

Ms. Patricia Kosseim: I'll ask Mâitre Caron to confirm, but my understanding is that our contact person for this investigation, particularly near the latter end of the investigation, was their legal counsel, David Fraser.

Mr. Bill Siksay: Is he based in Canada? Is he a Canadian?

Ms. Patricia Kosseim: Yes, he is based in the Atlantic region at McInnes Cooper.

Mr. Bill Siksay: Okay. Does he have particular responsibilities for Google around privacy concerns, or is he a legal counsel?

Ms. Patricia Kosseim: I don't know.

Mr. Bill Siksay: I know one of the things the commissioner has asked for is that by February those who are responsible be clearly designated and identified. Right now, is there anybody in Canada who's designated, other than the legal counsel, for privacy concerns?

Ms. Patricia Kosseim: Just to be clear, David Fraser is their external legal counsel. Maybe that's a question you can clarify with Google, so I don't misspeak.

Mr. Bill Siksay: Right. I was just getting at whether or not we will be hearing from the right person. You can't offer any other advice in that regard at the present time?

Ms. Patricia Kosseim: No, I'm sorry.

Mr. Bill Siksay: Okay.

The commissioner has done this investigation, made recommendations, and set a deadline, and she wants proof from Google that they've addressed the concerns she's raised. In a case like this, where an investigation's been undertaken and recommendations have been made, generally what's the next step? If there isn't compliance, what happens at that point? What are the consequences of non-compliance at this point of an investigation?

Ms. Patricia Kosseim: Mr. Chair, one of the powers she has under the current legislation, PIPEDA, is that at the end of her investigation, particularly if she recommends something the organization does not comply with, she has the option of going to Federal Court under section 15 of the act and taking the organization to court to have the court then adjudicate on the recommendations and to have those recommendations enforced by a judge.

Mr. Bill Siksay: So that would be the next stage in any case where there was non-compliance?

Ms. Patricia Kosseim: In any case it would be.

● (1645)

Mr. Bill Siksay: Okay, thank you.

Thank you, Chair.

The Chair: Thank you, Mr. Siksay.

We now go back to Madam Fry for five minutes.

Hon. Hedy Fry: Thank you very much.

I want to pick up on something my colleague Dr. Bennett said. She talked about the fact that parallel streams of technology move very quickly—both of us are physicians—and in medicine, that's the way it's happening. However, people who use that technology, such as physicians, automatically have an ethical code. The ethical code is for us to do no harm. I mean, the precautionary principle is built in to what we do.

Given that communications technology, and other technology, is moving along so very quickly—we're talking about what Google did—we should be thinking about what they could do. It was only within the last short period of time that they were actually able to develop the technology to get the Wi-Fi personal data information.

If you have companies that have the ability through technology to collect data or information or do things that could have potential harm, how do you build in some piece of regulation or legislation? Obviously companies aren't doing it. I don't want to beat up on Google, but the fact that they didn't stop to think and that it was considered superficial tells me they didn't believe this was worthwhile—that privacy is a superficial issue, and who cares?

How do we build in legislation that ensures there is some kind of ethical and precautionary regulation for companies that have access to harmful technology? And Dr. Bennett talked about the good that technology can do, and you have to balance it out. How do we build that into some kind of legislation or regulation that could say you've got to deal with precautionary principles, and as your technology moves so rapidly you've always got to consider what harm it can do? I'm here to tell you that if a physician or a radiologist used brand-new technology that hurt the patient, and they were taken to court, they couldn't say they didn't know. I'm sorry, that's not acceptable. You've always got to weigh the good plus the bad. There's lots of good in this technology, but harm has to be weighed.

Is it important to get that kind of regulation or wording in the law, and not just under the Privacy Act? I mean, this criss-crosses the communications act.

Perhaps your legal person might be able to answer this question better. What is it we, as legislators, can do when we see a loophole, an opening we haven't paid attention to, to make sure we protect and prevent future harm?

This technology is moving so fast. We're talking today...and tomorrow we might be talking about something totally different. Therefore, there has to be a precautionary principle involved.

Ms. Patricia Kosseim: I'll let Mr. Caron address that question.

Mr. Daniel Caron: I think the commission shares your concern with respect to how fast technology is emerging and the privacy implications of emerging technologies.

I'm not sure if I can specifically answer the honourable member's question, but I think one positive thing that has come out through our experience with the Personal Information Protection and Electronic Documents Act, PIPEDA, is that it has shown to be sufficiently malleable to deal with these emerging technologies.

It came into effect before the Facebooks and the Google Street Views. But as a principle-based act, it has shown to be quite flexible in dealing with new technologies and finding the right balance between allowing companies to offer innovative products but in a manner that also protects personal information—the privacy rights.

Hon. Hedy Fry: But it's a reactive act; it's not a proactive act. I'm talking here about proactivity as opposed to reactivity, where somebody does something and they are taken to court and you can do whatever you wish.

Again, I am not trying to cast aspersions on Google. But you sent a letter in June 2010 and you have not yet had an answer—it's November in two days—yet Google sees fit to speak through the media about this issue. I call that disrespectful. That's been a long time for this company not to at least send a preliminary letter saying they got your stuff, they're working on it, and they'll send another letter in two days' time. There has been this talking through the media, and an ignoring of a privacy commission who sent a letter to a company...was it four months ago? The media is getting all the answers. I find that disconcerting with regard to ethics.

● (1650)

Ms. Patricia Kosseim: Just to be clear, the letter that was sent in June notified Google that the commissioner was initiating an investigation. There has been active correspondence between the commissioner's office and Google representatives throughout the investigation process. She most recently sent them her preliminary letter of findings. I believe that was on October 14.

If I may add to Mr. Caron's answer to your question about PIPEDA, one of the ways the commissioners, acting together, encourage organizations to be more proactive is to take all those principles in PIPEDA and use them in a privacy risk assessment that they should carry out prior out to the deployment of technologies. We call that a PIA, a privacy impact assessment.

PIPEDA provides the tools and principles for any organization to be proactive in identifying and managing the risks before deployment, if they walk through the principles behind PIPEDA and do a proper assessment of the risks using the PIA process. It's done much like an environmental impact assessment. Those are the tools needed to avert the risks of new information technologies, which the commissioner is first to embrace as important and novel advances, as long as the privacy risks are being properly managed in the process.

The Chair: Thank you very much, Ms. Fry.

Madame Freeman.

[*Translation*]

Mrs. Carole Freeman: Thank you, Mr. Chairman.

We see that there is a consensus among parliamentarians. Ms. Davidson, Ms. Fry, Mr. Albrecht and Mr. Siksay mentioned that. We are really concerned about the situation, about what is going on with Google Street View and as a result of all the exemptions they had.

I have a completely different file in my hands. Germany and France are even considering banning Google because they think that really goes too far. I'm looking at all the countries. We are all watching and letting Google continue to act. What is our interest? I'm asking myself that question. Why can any technology emerge in this manner without us doing something else than stupidly looking at each other and letting people do things in their own way, cavalierly?

My second question is this: following all this uproar, Google decided to appoint Ms. Alma Whitten to the position of privacy policy officer. In fact, I believe she will be a scapegoat. She will try to manage the kind of monster that Google is, with all its tentacles. Does she have any training? Is she working with the commissioners of the various countries? What does this lady do?

I'll have a third question later. I don't know whether I'm going to have time.

Ms. Patricia Kosseim: I'll briefly try to answer your two questions.

I'll start with the second. I don't know Ms. Whitten. So I can't speak to that point. I don't know whether this is something new for her or whether she has previously been appointed. I can contact you again to forward that information to you, or perhaps you can put the question directly to the Google representatives when they appear. Once we have Google's response to our recommendation that a governance system be put in place, the commissioner will probably extend her analysis further and ask that kind of question to ensure the governance system is effective enough to manage these major privacy issues.

In response to your first question—

● (1655)

Mrs. Carole Freeman: In fact, that wasn't a question, but rather a comment. You don't need to respond. We feel overwhelmed by the situation. We no longer know where they're going to stop. We get the impression we'll never be able to fill the gaps that will be created. We all seem powerless, whether it be in Europe, Australia or elsewhere. They are all powerless. We are powerless and we let them act. I don't think this situation makes sense anymore. It's the same everywhere.

I'd like to go back to the situation we have in Canada. I know that Quebec, Alberta and British Columbia are not governed by the Personal Information Protection and Electronic Documents Act. Yesterday, my colleague Bill Siksay asked me a question in the House. He wanted to know what advantages the Quebec act had over Canada's legislation. Are you working jointly with the three provinces to achieve exactly the same harmonization?

Ms. Patricia Kosseim: The provinces you named have legislation that has been deemed equivalent.

Mrs. Carole Freeman: Do you mean they have been harmonized?

Ms. Patricia Kosseim: They have been deemed equivalent—not the same, but equivalent in terms of protection. With that certification, those provinces are exempt from the application of PIPEDA in their territories. The provincial act is recognized by an official process.

Mrs. Carole Freeman: I don't want to address matters from a legal standpoint because we don't recognize... We believe the federal government is interfering in this field. We believe that personal information is a provincial jurisdiction.

I won't retain the information you've just provided because it's contrary to the Constitution. I'm a lawyer. So we're going to agree on this point. We won't go into a legal debate.

I would simply like to know, with regard to content, how we are protecting citizens. You say it's equivalent.

Ms. Patricia Kosseim: There is close cooperation between the provinces and our office. We hold monthly conference calls to discuss common issues.

Mrs. Carole Freeman: Do I have any time left, Mr. Chairman?

The Chair: You have time to ask a very brief question.

Mrs. Carole Freeman: I believe Canpages was sold to Yellow Pages. Was there a transaction?

Ms. Patricia Kosseim: I don't know.

Mrs. Carole Freeman: That's fine. Thank you.

[*English*]

The Chair: Thank you, Madame Freeman.

Mr. Siksay, you have five minutes.

Mr. Bill Siksay: Thank you, Chair.

I want to come back, probably to Maître Caron. In response to an earlier question about the recommendation to delete the information that was being held, you explained that this was being delayed because of some U.S. civil actions related to the collection of the data in the first place.

I want to be clear. The payload data and the Wi-Fi access-point data that Google collected in Canada are now being stored in the United States, and not at all in Canada. Am I correct about that?

Mr. Daniel Caron: That's right. The data is being stored in the U. S.

Mr. Bill Siksay: Are we aware of any Canadian litigation related specifically to the collection of that data?

Mr. Daniel Caron: To my knowledge, there isn't any civil litigation with respect to that matter.

Mr. Bill Siksay: And the Canadian data is separate from the U.S. data. They're not all jumbled up together? The data collected in Canada is identifiable, as is the data collected in the United States? Am I correct about that as well?

Dr. Andrew Patrick: You are, except that there were some slight issues that arose when they drove near the border.

Mr. Bill Siksay: Okay.

I'm just wondering why there is a delay. If the commissioner's recommendation was that the information be deleted and we're not aware of any Canadian litigation, why are we waiting to have the Canadian data deleted, or why is there any delay in that process?

Mr. Daniel Caron: I think it may have to do with the data my colleague just spoke about. Some of that data might be relevant to some of the ongoing civil actions that have been consolidated in the U.S. So out of an abundance of caution, we didn't want to recommend that Google destroy data that might be relevant to ongoing proceedings.

Mr. Bill Siksay: Now what about the data related specifically to border areas?

Mr. Daniel Caron: There might be information relating to the Wi-Fi incident that might be relevant to ongoing U.S. proceedings.

Ms. Patricia Kosseim: I think it has to do with the border but also with communications between Americans and Canadians that may involve e-mail correspondence or communications from individuals on both sides of the border. So it may be difficult, within e-mail correspondence, for instance, or within communications between a Canadian and an American, to perfectly segregate only the U.S. data from the Canadian data. Those are the kinds of complications that need to be worked out.

● (1700)

Mr. Bill Siksay: But if the Canadian data were stored only in Canada and not transferred out of the country and stored in the United States, would we have this problem? If Google had kept all of that data here in Canada, we'd be able to say, "That's the Canadian data. There is no litigation involved in this. Delete it now." Am I correct about that? Is this a problem that's arising because we're allowing Canadians' personal data, which was gathered here in Canada, to be transferred and stored outside of the country?

Ms. Patricia Kosseim: I can't answer with certainty, but I think the laws of evidence would need to be considered. So regardless of where the data is stored, if it involves evidence for the ongoing class action suits in the U.S., there are obligations not to destroy the data, whether you store it in Canada or in the U.S. I think those are the kinds of subtleties the commissioner wanted to be sensitive to.

Mr. Bill Siksay: So Canadians would have those obligations to a U.S. court action? That's what's confusing me. This is data that's Canadians' data. It's collected in Canada. Would we be responsible for protecting evidence that Americans might think they need at some point, even though it all pertains to Canadians and was collected here in this country? I don't think we would normally be in a normal court situation. I'm not a lawyer.

Ms. Patricia Kosseim: I can't answer with certainty, but it has to do with cross-border instances when there may be a mingling of the data and correspondence between Americans and Canadians such that you cannot segregate correspondence for just the U.S. portion or just the Canadian portion. So it has to do with that.

Mr. Bill Siksay: Do other U.S. agencies, like Homeland Security or the FBI or the CIA, have access to this data now that it's stored in the United States? Would they have access, given that this data has left Canada? I know we raised concerns about the actual photographs being stored in the United States and privacy concerns around that. It seems to me we've taken a further step with private correspondence, e-mails, that kind of thing, what we're accessing on the Internet now going out of the country and being stored there. It seems to me that we've raised the level of privacy concerns significantly. So do any of those agencies have access to that data now that it's in the United States?

Ms. Patricia Kosseim: I'll let Mr. Caron answer that question.

Mr. Daniel Caron: I guess personal information that is stored in any country is subject to the laws of that country. So it would be possible in certain circumstances for some U.S. agencies to have access to that information.

Mr. Bill Siksay: Which they wouldn't have access to if that information had been kept and stored here in Canada.

Mr. Daniel Caron: They would have access to it by virtue of being President of the United States, for example.

Mr. Bill Siksay: So if the data collected in Canada had never been transferred to the United States, they might not have access to it here.

Mr. Daniel Caron: I can't fully answer that question.

The Chair: Thank you, Mr. Siksay.

There are a couple of points I want to cover, Madam Kosseim.

First of all, on Wednesday the Federal Trade Council in the United States issued a two-page ruling on this issue chastising Google but without sanctions. Insofar as you're aware, is this the end of the regulatory issue in the United States?

Ms. Patricia Kosseim: I believe that was a letter from the Federal Trade Commission.

The Chair: Yes.

Ms. Patricia Kosseim: Interestingly, it's echoing the same messages the commissioner gave Google and saying that in their view, given the recent indication of Google's response to the recommendations, which the commissioner also made, they felt confident they could stop the inquiry on that basis.

The Chair: To summarize what you're saying, I believe you testified that a number of civil actions are going on against Google, but as far as being a regulatory issue, the investigation was started but it's been concluded.

Ms. Patricia Kosseim: This is just one regulatory body, the Federal Trade Commission. There may be the FCC, Federal Communications Commission. I understand there may also be attorneys general of 38 states or more who have come together and are inquiring further into this incident to determine what action, if any, they will also be taking. So this is just one regulatory agency.

● (1705)

The Chair: Mr. Caron, are you aware of other regulatory matters going on?

Mr. Daniel Caron: I'm aware of the fact that a request has been issued to the Federal Communications Commission, and as Mrs. Kosseim mentioned, 38 attorneys general are looking into this.

The Chair: The last issue I want on the record is whether the Office of the Privacy Commissioner is satisfied at this time that the Google street view application itself as well as the Canpages' street scene counterpart sufficiently protects the privacy rights of Canadians and what, if any, are your outstanding privacy concerns?

Ms. Patricia Kosseim: With regard to the street view imaging technology by Google and Canpages, one point I just want to clarify is that those were never the subject of an investigation by the commissioner. Those were dealt with by correspondence between the commissioner and the organizations. So the extent of what we know is not as in-depth as it would have been had there been an investigation into those matters.

But on the basis of the correspondence and the response of the organizations, there has been a lot of movement on the part of both organizations to comply with or to move along in harmony with the recommendations the commissioner has made, including notification to neighbourhoods before they arrive, discussions with vulnerable stakeholders and groups, take-down procedures, retention and deletion mechanisms, and other such protections. So on the basis of that correspondence there's been a lot of movement. Of course there could always be improved notification, and there could always be ongoing improvements to blurring technology, but so far there's been great improvement and movement toward the commissioner's wishes.

The Chair: Colleagues, I believe that's the end of the rounds. That's the end of questions, I believe.

I'm going to ask you, Madam Kosseim, if you have any concluding remarks for this committee. Do you have any closing remarks you want to make or leave us with?

Ms. Patricia Kosseim: In summary, I think the important point has already been made. And I thank all members for having given us the opportunity, on several occasions, to repeat the key message, which is our hope that organizations, in conceiving, developing, and deploying information technologies from which we, as Canadians, all benefit take the proactive measures up front to identify the risks, assess them, and manage them before deployment of these technologies on a widespread basis. I thank you for the opportunity to say that.

The Chair: On behalf of all the committee members, I want to thank you. I think all members of the committee are probably confused and at the same very concerned about what's going on. I have a suspicion the world of technology is moving faster than we're moving. But again, it's our job, perhaps, to catch up.

That being said, I want to thank you again for your excellent work. I want to thank you for your appearance here today.

The next meeting is Tuesday at 3:30.

The meeting is adjourned. Thank you.

MAIL POSTE

Canada Post Corporation / Société canadienne des postes

Postage paid / Port payé

Lettermail / Poste–lettre

1782711
Ottawa

If undelivered, return COVER ONLY to:
Publishing and Depository Services
Public Works and Government Services Canada
Ottawa, Ontario K1A 0S5

En cas de non-livraison,
retourner cette COUVERTURE SEULEMENT à :
Les Éditions et Services de dépôt
Travaux publics et Services gouvernementaux Canada
Ottawa (Ontario) K1A 0S5

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

SPEAKER'S PERMISSION

Reproduction of the proceedings of the House of Commons and its Committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the *Copyright Act*. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a Committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the *Copyright Act*.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its Committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this 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

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la *Loi sur le droit d'auteur*. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la *Loi sur le droit d'auteur*.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

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