HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 041 • 1st SESSION • 41st PARLIAMENT

EVIDENCE

Tuesday, May 29, 2012

Chair

Mr. Pierre-Luc Dusseault

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, May 29, 2012

● (1135)

[*Translation*]

The Chair (Mr. Pierre-Luc Dusseault (Sherbrooke, NDP)): Good morning, everyone. Since we have quorum, we will start. Welcome to this very first meeting to study privacy and social media.

I am pleased to have with us Ms. Stoddart, the privacy commissioner.

First, I would like to ask committee members whether they agree to extending this meeting by half an hour, given the vote in the House and the fact that several witnesses who will appear before us will want to be able to speak and answer questions. Do we agree to extending the meeting by half an hour?

[*English*]

Mr. Dean Del Mastro (Peterborough, CPC): I would move if I could, Mr. Chairman, that perhaps we reduce the period of time for each group of witnesses to 45 minutes, which would allow us some time for committee business at the end.

[*Translation*]

The Chair: If the committee agrees, we will take a little less time for asking questions, but the witnesses will each still have 10 minutes to make their presentations. So there will be fewer questions if that is the committee's wish. We will also have to set aside 10 minutes at the end of the meeting, after the witnesses have left, to discuss a few important things for the committee and to be able to plan the rest of the study.

Mr. Angus, do you want to take the floor?

[*English*]

Mr. Charlie Angus (Timmins—James Bay, NDP): I'm asking the indulgence of my colleagues, because I was surprised that when we asked for the report from Madame Benoit, later on we were told that it was under a cloak of confidentiality. That was not my understanding.

I know we have committee business, but at the beginning of this meeting I want to be clear that when someone presents us with a report we've asked for, if there is a reason for it to be confidential then we will respect that, but something that looks as though it was put together using Google pictures, I think, has no reason to be kept under confidentiality.

I'd like to ask if I could get unanimous support, since we have media here and people want to know what's in that report, for it to be released to the media, and then we can carry on with our business at the end of the meeting.

[*Translation*]

The Chair: This has to do with a whole other topic, but since Mr. Angus is asking for unanimous consent, I just want to remind committee members that there was a letter from—

[*English*]

Mr. Dean Del Mastro: Can we deal with the matter on the floor first, and then we'll come to Mr. Angus' motion?

[*Translation*]

The Chair: The motion regarding the 45 minutes has already been accepted. There never really was a motion; agreement was unanimous.

[*English*]

Mr. Dean Del Mastro: Was that agreed to? Okay.

On Mr. Angus' motion—

[*Translation*]

The Chair: I would just like to clarify one thing: we received a letter from Ms. Benoît's assistant, Ms. Pérusse, who said that the documents were confidential. Since I am at the service of the committee, if you decide otherwise about it… It is your decision, but I just want to remind you that we were clearly told that it was confidential.

Mr. Del Mastro, do you want to take the floor?

[*English*]

Mr. Dean Del Mastro: I'd just say if it was intended to be confidential, it's not. I'm sure most members read the story in the *Globe and Mail* this morning.

I don't see any reason why this should be held confidential either. We had hearings here that were entirely in public. We heard testimony that was entirely in public. I think secondly there were a number of questions that were either not answered or perhaps not answered fully.

I'm entirely supportive of what Mr. Angus is requesting. I would anticipate most members here at the committee would be.

[*Translation*]

The Chair: The clerk told me that he spoke to Ms. Benoît today and that she has several concerns. Of course, she had already told us that it was confidential for a number of reasons that will perhaps be explained to us a little later. Since the company operates in the private sector, we may perhaps understand that she does not want to share the information with everyone.

Furthermore, since it is the committee's decision, I can do nothing to stop you, either. It is up to the committee to decide.

Mr. Angus?

● (1140)

[*English*]

Mr. Charlie Angus: With all due respect, I think it's very important to have this on the record. We in the official opposition take the rights of the witness very seriously. This is not meant to be a kangaroo court. There were many concerns about why taxpayers paid money for that trip. We had asked for answers. We had asked for the report.

If the report had supplied the kind of information on meetings or perhaps on costings or other things that would have been shared with the various ports in Australia and the Port of Montreal, that would be an issue of confidentiality we would be bound to respect.

I'm very concerned that someone has presented this report and then after the fact has claimed confidentiality. There's nothing on that report that even says confidential. There's nothing in that report other than something one could hire an intern or ask an intern to find on Google and Flickr. It seems to me we're being asked to use confidentiality perhaps to be almost like a cover-up.

I think that's not the role of our committee. I think the public should be able to see it, and the public should be able to make up their minds. I think it's our job to release that report.

[*Translation*]

The Chair: Mr. Del Mastro, you have the floor.

[*English*]

Mr. Dean Del Mastro: Thank you very much.

Again, with respect to the concerns voiced that this is somehow a confidential report, I haven't seen much that indicates it's in any way confidential. In fact, it's as I suspected when the witness appeared before committee. I did suggest there was nothing in the report that you couldn't get off Google.

I also suggested that while she wouldn't respond to my direct question about how much she is paid in her position, which I think people in the public employment.... And with respect to your indication that they have private competitors, two thirds of their funding directly comes from the Canadian taxpayer. I think you have to respect those dollars, and you know frankly, I would simply argue that I don't see anything here that's confidential.

In my view, this was a personal vacation that was in part paid for by Canadian taxpayers, and I'd like Canadians and others to look at it and make that determination for themselves.

That's my determination at this point, and frankly, I think this committee should come forward with a report or at least a motion that we find this spending inappropriate, and that we seek that the government respond formally to what we've witnessed here and table that response in the House of Commons. I think that's where this should go.

[*Translation*]

The Chair: Thank you.

Some witnesses are appearing as part of another study. Several things have been said, and I expressed some reservations. Everyone seems to agree on continuing the work. Is there unanimous consent? That's basically the case.

As for Ms. Benoît's documents, we would have to consult the clerk to determine how to distribute them. The documents are lengthy and cannot be sent by email. We will see what can be done.

Mr. Del Mastro?

[*English*]

Mr. Dean Del Mastro: Thank you, Mr. Chairman.

I could simply move a motion in addition to Mr. Angus' motion on which I do believe you have unanimous consent, which is to publicly release the report. I would also like to move that you table the report in the House of Commons, and that we request a response from the government in this matter.

[*Translation*]

The Chair: I'm at the service of the committee. Would the committee like to proceed this way? Do we have unanimous consent?

The clerk is suggesting that a motion be drafted and worded in a way that is acceptable to the House of Commons, so that it can be moved at the next meeting and formally adopted. There seems to be unanimous consent. So we can move on to today's agenda.

Thank you, once again, Madam Commissioner, for being with us today. You have 10 minutes for your presentation. We will then have a period of questions. I will remind committee members that they must address their comments through the chair, as usual.

Madam Commissioner, you have the floor.

● (1145)

[*English*]

Ms. Jennifer Stoddart (Privacy Commissioner, Office of the Privacy Commissioner of Canada): *Merci*. Thank you very much, Chair and honourable members, for the invitation to appear before your committee today as you begin your very important study on social media companies and the steps they are taking to protect the personal information of Canadians.

I'm joined here by two social media experts from my office, Daniel Caron, legal counsel, and Barbara Bucknell, policy analyst, on this issue.

I'd like to start by giving you a brief overview of social media. I'm sure you've now all had experiences with these online platforms. They've become important channels for news, for communications, relationships, the sharing of photos, videos, and almost anything else that can be digitized. That said, I think it is useful to start with an overview of the industry to help clarify what it does and how its activities have an impact on the privacy of Canadians.

Social media involve applications that allow individuals, organizations, and communities to share information and to generate content. Building on traditional business models where businesses required personal information in order to provide a service, today individuals young and old voluntarily share their personal information on social media sites to connect with other people, or in some cases, to draw attention to themselves and to their views. Indeed, many social media sites encourage users to establish profiles that reflect who they are, what they are interested in, who they know, and what they like. Many provide their services for free in the hopes of gaining a larger user base.

To suggest that these services are "free" however is not entirely accurate. Social media companies can quickly amass a staggering amount of personal information. In addition to the preferences, habits, and social interactions of their users, these companies also collect vast amounts of background information that is not visible on public profiles, including search histories, purchases, Internet sites visited, and the content of private messages. This collection of billions of data points allows social media companies—using sophisticated algorithms—to analyze user behaviour in order to refine their services, and to identify ways to generate revenue. It can also enable others, such as researchers, employers, school administrators, and law enforcement, to learn more about individuals and their activities.

This is the age of big data where personal information is the currency that Canadians and others around the world freely give away.

[*Translation*]

My office has a mandate to ensure private sector compliance with the Personal Information Protection and Documents Act, which applies to the commercial use of personal information by social media companies operating in Canada.

Over the course of the past five years, we have engaged with, and conducted investigations into, many players in the industry, both big and small. A significant part of our recent research and policy work has focused on understanding and explaining to others the privacy implications of the social media phenomenon.

Ever mindful of the importance of innovation in today's digital economy, we have tried to strike a reasonable balance between companies' desire to experiment with new products and services, and an appropriate level of protection of Canadians' personal information.

[*English*]

That said, I have become very concerned about the apparent disregard that some of these social media companies have shown for Canadian privacy laws. Although we've made some headway with some of these campaigns, I would like to identify the following significant privacy concerns that I believe require more attention on the part of all social media sites, and these are the four following issues: accountability, meaningful consent, limiting use, and retention.

I'll start with accountability. Too often we have seen privacy concerns being addressed after a major problem is uncovered or there is a backlash on the part of users. While it appears that many of the major players are making improvements on this front, the social media world is constantly evolving with new entities popping up regularly in a hurry to get their new service on the market. Privacy does not appear to be a top priority for them.

● (1150)

This is one of the reasons that my office, together with my counterparts in Alberta and British Columbia, recently issued accountability guidance to companies on the internal privacy processes and procedures that need to be in place, including having an individual in charge of privacy.

Second, the issue of meaningful consent is critical. Social media companies need to clearly explain the purpose behind their collection, use, and disclosure of personal information, and what third parties, such as application developers, they are sharing this information with. And they have to clearly obtain users' consent.

This is a particularly challenging issue, since privacy policies tend to be too long, too convoluted, and largely ignored by users. Providing adequate information, which users can easily understand, read, and consent to, is a challenge for social media companies and data protection authorities.

Further complicating the issue of consent is the fact that children are online from an increasingly young age. The youngest users may not yet be able to provide meaningful consent required under PIPEDA.

[*Translation*]

The third issue is limiting use. Social media services are constantly evolving in an effort to be innovative and competitive. This has meant that personal information can be used in new, and sometimes, unexpected—even unwelcome—ways. It is important to keep users properly informed, explaining new features in a timely fashion, and seeking their informed consent for new uses of personal information. I think we also need to learn more about how personal information on these sites could be used, beyond advertising, and the onus should be on social media companies, as with all other organizations, to be fully transparent about their personal information practices.

The fourth issue of concern is organizations failing to establish retention schedules of personal information and true deletion options for individuals. Social media companies need to be clear about how long they retain the personal information they are collecting. They should also spell out how they treat personal information differently when an account is de-activated versus when an account is actually deleted.

Under the Personal Information Protection and Documents Act, firms are obliged to keep data only as long as is necessary for a specific purpose and then they must destroy it. Vast quantities of data, often located in other countries, can also pose security issues.

[*English*]

Honourable members, as you proceed with your study into privacy and social media, you may wish to use these principles—that of accountability, meaningful consent, limiting use, and retention—as a guide for assessing how social media companies protect the personal information of Canadians.

In conclusion, Mr. Chair, in public opinion polling commissioned recently by my office, we asked more than 2,000 Canadians about social media, and 83% of respondents said online companies should be asking for explicit permission before tracking their Internet usage and behaviour. Clearly, Canadians value their online privacy. That's why we feel it is so important to hold companies to account for how they collect and use personal information.

To that end, we have made steady progress with the tools available to us under the present law, but I believe much more needs to be done. The reach of digital companies using Internet and mobile technologies to collect and share personal information will only grow in the coming years.

My office has been conducting extensive research and analysis in preparation for the second mandatory five-year review of PIPEDA by Parliament, which is now past due. We're giving serious thought to how the current regime, which predates all these novel technological developments, should be modernized to keep up with the times. Top of mind is how the existing enforcement powers could be further strengthened to curb industry non-compliance and encourage greater accountability from companies for the personal information they collect, use, and share with others.

In recent years there has been a trend internationally toward more robust enforcement powers. Canada has long been a leader in terms of privacy protection laws, but I believe we now risk falling behind.

I look forward to sharing my office's detailed position on this matter when the parliamentary review gets under way.

● (1155)

Thank you very much for the time, Mr. Chair. I would be happy to answer any questions the honourable members have.

[*Translation*]

The Chair: Thank you for your presentation.

Since we are short on time, we will have five-minute periods to allow as many people to speak as possible.

Mr. Angus.

[*English*]

Mr. Charlie Angus: Thank you, Mr. Chair.

Thank you, Madam, for coming. I'm very pleased that you are our first witness, because your office is one of the few recognized beacons out there dealing with this issue.

I think, from a legislative point of view, there were many years where we felt that it was probably dangerous for politicians to step in on this emerging technology, because we didn't know where it was going. We had to allow this market to develop. We had to allow the technology to come of age. Suddenly it came of age, and very quickly; it moved faster than any of us ever conceived. We feel we're playing catch-up.

In terms of the issue of privacy in particular, people are now living almost entirely online, and there are enormous implications. Social media is an incredible force for good and for communication, but there are issues of privacy, security, safety. There's a whole manner of issues that we have not even begun to get our heads around.

In the short time I have, I'd like to focus on your four main points: accountability, meaningful consent, the limitation of use, and retention of data.

In terms of the issue of accountability, we have government legislation with PIPEDA coming forward, yet in this law, when they're looking at the issue of the breach of privacy, the onus is on the company to decide whether or not to share that with the citizen. It's based on the issue of significant risk or harm.

Do you believe we need to have a clearer standard? I cannot imagine a company ever calling its consumers and saying, “Guess what? Someone has been breaching our data, but don't worry; stick with us.” The obligation of the company to the consumer I think should outweigh the risk to its bottom line, because at what point is the consumer going to be able to be assured that their privacy is being respected? What role do you think your office plays, and what role do you think should be the standard, for issues of breach of privacy?

Ms. Jennifer Stoddart: Thank you for the question, honourable member, on a very important topic—namely, the growing threats to data security throughout the world but including, too, the information held by Canadian companies or of Canadians elsewhere.

In this area, once again Canada has lagged significantly behind. We don't have specific data breach provisions. I believe we should. I believe we also have to couple them with some kind of incentive for companies to invest in the appropriate data security standards.

There is some legislation currently at second reading. I think the standard in the legislation is acceptable. It mirrors that which was already adopted by Alberta. But I think we have to have stronger enforcement powers, because under the present regime there's almost no sanction for a company that doesn't report either to my office or to consumers, if there's a real risk of significant harm.

So I would welcome this issue being re-examined.

Mr. Charlie Angus: The issue with Facebook going with its public offering and the share price crashing.... Everybody I know is on Facebook. I live on Facebook. There will be enormous pressure at the company level since the market decided that its advertising model may not be what they thought it was. Their other incredible treasure trove is the data, and there could be increasing levels of pressure now that they're in a public offering to open up that data.

In terms of the limitation of use, how do we set down some basic rules that need to be enforced? Are there issues of “do not track”? Have you thought of what it would look like to lay down some rules in terms of protecting that data from unfair exploitation?

Ms. Jennifer Stoddart: Yes. In fact, we've been almost continually investigating Facebook since about 2009. There are clear rules. We have intervened time and time again to check as to whether or not Facebook was following these rules. The first time they weren't. In subsequent investigations, it seems they had a higher level of compliance.

The problem with social media companies is generally their lack of transparency with regulatory authorities. It takes a very skilful investigation, with a lot of experts, particularly in information technology, in order to find out really what they're doing.

● (1200)

Mr. Charlie Angus: I guess the issue is meaningful consent, because there are mechanisms on all the various sites to allow you certain privacy settings. But as they say, the devil's in the defaults. Is that something we should be looking at in terms of coming up with recommendations or legislation? Should the opt-out mechanism be there so you get to make that choice clear and upfront, and so you know what you're signing on for?

Ms. Jennifer Stoddart: I would welcome this committee looking into privacy policies. Over the years, we've said they have to be clearer, they have to be readable, so that people really understand.

Again, unless we're in an investigation and we say you modify this policy so that it's a lot clearer to a user or we will have to take further steps, which involves going to federal court, in my experience, as we go online, once again, we see unreadable privacy policies. That says to me that companies are only making clearly worded privacy policies for the consumers when they're forced to. Otherwise, it's in legalese that even lawyers have difficulty following, and it says if you have a problem, go to the courts of northern California.

This is not acceptable.

I would welcome this committee examining this problem more closely.

[*Translation*]

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

Mr. Del Mastro now has the floor.

[*English*]

Mr. Dean Del Mastro: Thank you, Mr. Chairman.

Thank you to the witnesses today.

It's very interesting testimony. You indicated, Ms. Stoddart, that we live in the age of big data, and I think it's actually remarkable. Mr. Angus talked about the short time period in which this has evolved. I think companies have been studying consumer behaviour for generations. They test-market things, and in fact, Peterborough was long a test market community for various products. They don't do that much anymore, because they are working off data that they are actually gleaning.

You talked about the algorithms and so forth that they use to determine consumer approval or consumer likes and dislikes. You also talked about how Canadians, but also people around the world, give this information away freely, and about actual informed consent.

It seems to me that when you go to sign up for any of these sites—and I've signed up for them myself—they have a very long legal agreement that I would argue is beyond the comprehension of many people using the sites, especially young people, especially very young people. Should there be almost a disclaimer that says, “We are going to study what you are doing. We are going to note where you go. We're going to use these observations to report back to firms that will pay us for this information. Do you consent to that?”

Would that be a real simple way of putting it out in just basic English as to what their end is? We know what people's ends are. If you go to Facebook, it's one of the greatest communication tools. YouTube and so forth, these are incredible tools. Frankly, like a lot of people, I really like them. But their end in providing it is that they are gaining value out of it, correct?

It's not well understood, the value they're gaining from people. You indicated this information, big data, is something people are giving away freely. It's not being resold freely or repackaged freely.

Ms. Jennifer Stoddart: Very simply, honourable member, I agree with your suggestion. Exactly. You have to talk to people clearly. That's not what's being done.

Mr. Dean Del Mastro: Bill C-29, which was in the former Parliament, made some changes to PIPEDA, and Bill C-12, which was reintroduced on September 29, 2011, had a key amendment that required organizations to report data breaches—referred to in the bill as breaches of security safeguards involving personal information—to the Privacy Commissioner and notify affected individuals when there is real significant harm, such as identity theft or fraud.

I have a lot of folks in my community who are concerned about identity theft. It seems that every once in a while we'll hear about a significant security breach. In fact, your office has reported on some of them. This reporting requirement for security breaches, is it something you would support, these changes that are suggested in Bill C-12?

Ms. Jennifer Stoddart: Yes, honourable member. I think the changes that Bill C-12 would bring are very welcome, but I don't think they go far enough. We're now halfway through 2012, and as I mentioned in my presentation, Canadian privacy legislation has lagged behind the reforms in other major countries, and so there isn't much incentive for corporations to invest in the kind of software or personnel training that makes Canadians' data safer. So I think basically the bill could be strengthened.

● (1205)

Mr. Dean Del Mastro: I think it's a double-edged sword. People value their privacy, but at the same time I find it very surprising the things that people will put out about themselves on Twitter, on Facebook, on any of the social media sites. But then they'll turn around and say, “Hey wait a minute, this is an invasion of my privacy.”

It seems that people are prepared to broadcast details of their lives and so forth to almost anyone who wants to see it.

Is there a bit of hypocrisy here? Are we, on the one hand, concerned about what might be done with personal details, while there's this other rush to push things out and to interact with as many people as possible? It seems that there's an irony here.

Ms. Jennifer Stoddart: Yes, I believe you're absolutely right, honourable member. We're dealing with human nature. We're dealing in an individualistic society, with everyone's different opinions of privacy depending on the context in which they find themselves. What I may say in one forum, like here, is not what I might say to my best friend over dinner.

The advent of new technology has changed those contexts, so people will react in very different and perhaps contradictory ways. This technology is also very new, so we don't know how much of our behaviour online will change over time, as we become older, go through various life experiences, and so on. Those are things that have yet to unfold.

But yes, there's a wide variety of behaviours online.

[*Translation*]

The Chair: Thank you. Your time is up.

Mr. Andrews has the floor for five minutes.

[*English*]

Mr. Scott Andrews (Avalon, Lib.): Thank you, Mr. Chair.

Thank you, guests, once again, for coming in.

On the issue of retention, exactly how long are these companies retaining this information? When someone decides they no longer want to participate and they shut down their account, I think there were two examples you used: deactivating it versus deleting it.

How long are these companies holding this information? How do we know they're actually destroying it in a manner that's acceptable, or do we not know that?

Ms. Jennifer Stoddart: Thank you for that question.

In fact there may be no limits as to how long many companies keep information, and that is one of the challenges. We are presently investigating a company—we finished the investigation—that had no plan to delete the information. It had information from users, and these were quite young users, from five or six years ago.

When we said that under the terms of the law they had to delete this, they said they couldn't because it wasn't written into their programming. This is a very serious issue. We're presently discussing with them as to what alternatives can be taken.

It varies according to company, but this has been a consistent issue. That's why we highlighted to this committee that there are not appropriate plans to delete the information, and there is not a clear explanation as to whether deactivating your account means your information is deleted or just not accessible.

Mr. Scott Andrews: How does an individual know their information was not deleted? One would assume that it has been. What would trigger them to say, hold on a second, they didn't delete my information? Would the user have any idea?

Ms. Jennifer Stoddart: I don't think they would, but could I ask Ms. Bucknell, who has worked on a lot of these investigations?

Ms. Barbara Bucknell (Strategic Policy Analyst, Legal Services, Policy and Research Branch, Office of the Privacy Commissioner of Canada): Thank you. In many of the cases we've seen, the individual has been able to get back on to their account, and that's how they knew that their information, which they had asked to be deleted, hadn't in fact been deleted. Then, they filed complaints with us.

● (1210)

Mr. Scott Andrews: Okay. Ms. Stoddart, when you look at different jurisdictions—these are multinational companies operating in different countries, different states—exactly how do we harmonize all the privacy laws?

One would think you would want to have it harmonized to some extent, because how do these companies actually say different jurisdictions have different privacy laws? How do we square that circle?

Ms. Jennifer Stoddart: Thank you. That's a very important question for privacy commissioners throughout the world. In fact, the privacy laws are not all that different. They are all based on the OECD fair information principles of 1980.

We, in Canada, chose to follow the European standard of privacy laws, and therefore we're adequate for the purposes of transferring data.

More recently there have been very positive developments in the United States, led by the Department of Commerce and the Federal Trade Commission, to make the privacy standards in the United States more explicit. There is very little difference now between the various countries.

Secondly, I'd like to add that privacy enforcement authorities are increasingly working together.

Mr. Scott Andrews: On April 4, your office released its statement about the investigation of Facebook, and it stated that they had agreed to make a number of changes. How do you know that these companies actually make the changes? They may just simply agree with you. How will you know that these changes were actually implemented?

Ms. Jennifer Stoddart: In fact, a while ago I announced a new policy, which was rather than have the taxpayers fund civil servants to follow up on the companies as to whether or not they'd actually done what they were supposed to do, we have asked the companies to go now and get a third-party audit by an accounting firm or a law firm, or something like that, and report back to us within a given time period that these changes have actually been done.

Mr. Scott Andrews: How has that process worked? Have you had any of those audits or third parties come back to you yet?

Ms. Jennifer Stoddart: We're waiting for two. One was an audit of Staples, which showed that Staples had persistent problems in deleting personal information from recycled equipment. That is due this summer. We have one from our last investigation of Google Wi-Fi, which was due in May. They're going to be late with it, to my disappointment. They're going to give it to us in July.

[*Translation*]

The Chair: Unfortunately, your time is up, Mr. Andrews.

[*English*]

Mr. Scott Andrews: Just one quick one. Did they give you a reason why they were going to be late?

Ms. Jennifer Stoddart: No, I don't think there was a clear reason.

[*Translation*]

The Chair: Ms. Davidson now has the floor.

[*English*]

Mrs. Patricia Davidson (Sarnia—Lambton, CPC): Thank you very much, Mr. Chair, and thanks, Commissioner, and the rest of your contingent for being with us again today. Certainly this is an extremely interesting study, and you were referring back to the Wi-Fi study that we did previously.... All of those certainly proved to be very interesting and hopefully what we've been doing will be in the better interests of the general public

I was interested when you talked about the privacy standards internationally. I think you had indicated that now they've been progressing and there's very little difference in the standards today. But in your opening remarks, you talked about the enforcement powers and how you felt that Canada could be falling behind. Could you elaborate on that a little bit more, please?

Ms. Jennifer Stoddart: Yes. Unlike most other major jurisdictions now, Canada has no major sanctions for those who don't follow its commercial privacy law. I hope that when the second five-year review of PIPEDA will be undertaken by Parliament this issue could be discussed. I believe companies take notice—and I'm talking about very large international companies that operate on a very large scale—when they are subject to major fines or some kind of enforcement action. We have very limited power in that regard, and I believe that more respect would be shown to Canada's laws if we did have that power.

Mrs. Patricia Davidson: And monetary sanctions are the norm in the other international countries, are they?

Ms. Jennifer Stoddart: They are.

Mrs. Patricia Davidson: Are there any other areas, when we're talking internationally, that we cover and they don't, or that they cover and we don't? Are there other important areas that we should be looking at as well as the enforcement?

● (1215)

Ms. Jennifer Stoddart: Yes. There's a whole other series of issues that you could look at in a PIPEDA review. I believe we will be releasing a paper on that very soon. Some of them are more details in working with the law over the years. Some are more major things like enforcement powers, the role of the individual in trying to enforce his or her own rights, which I think would be a good subject for study for this committee.

Mrs. Patricia Davidson: In your opening remarks, you talked about the provinces. You said that your counterparts in Alberta and British Columbia had recently issued accountability guidance to the companies, but there are more than two provinces that have legislation, are there not?

Ms. Jennifer Stoddart: Yes. In terms of regulating the commercial private sector, there's also the province of Quebec, which adopted a law in 1995. I believe Quebec did not choose, on the advice of its justice department, to join us in that document, although I believe they're planning to join us in issuing other guidance of another kind.

Mrs. Patricia Davidson: Are there only the three provinces?

Ms. Jennifer Stoddart: That's right. There are only the three provinces. Elsewhere in Canada, PIPEDA applies to commercial use of personal information.

Mrs. Patricia Davidson: Other than that change do they fall in line with each other pretty well? Are they comparable in the three provinces?

Ms. Jennifer Stoddart: Yes. Over the time I've been Privacy Commissioner, we have made it a priority to coordinate our efforts on messaging. We're producing joint materials more and more. We've done joint investigations. We think it's very important in a federated country like Canada that industry has a similar standard to observe throughout the country.

I think we've been fairly successful at ensuring that.

Mrs. Patricia Davidson: Do you think there have been any changes by the companies in the way they handle the personal information in these online sites? We hear more about it all the time with more concerns being raised. Is it just that people are becoming more aware of what can happen, or is there a difference in how they're handled?

Ms. Jennifer Stoddart: I believe there's a more creative use on that, but once again could I ask Ms. Bucknell to complete my answer?

Ms. Barbara Bucknell: I think people have become more aware, partly due to breaches and things like that, partly also due to some of these very large companies trying things with their membership, with the users who belong to their sites, and then getting user backlash in many cases.

We've seen that hit the news in a big way, particularly about two years ago. I think in that sense, yes, we hear a lot more about it, but they are always finding new, innovative ways to use personal information.

Mrs. Patricia Davidson: Are there specific challenges—

[*Translation*]

The Chair: Your time is up, Ms. Davidson.

Fortunately, we will be able to hear from more witnesses a little later.

Madam Commissioner, we are out of time to ask you questions. But we will continue this study for some time, and we will be able to ask you back to take stock of what was said by other witnesses, depending on the committee's wishes.

We need to suspend for a few minutes to make way for the next witnesses. There will then be 10 minutes for presentations and a few minutes for questions. We will have time to discuss committee business a little later.

Thank you.

● (1215)

(Pause)

● (1220)

The Chair: We are resuming the meeting as quickly as possible, given that we are a little short on time today.

I would like to thank the next witnesses from the Department of Industry for being here today. They have 10 minutes for their presentation. We will then have a period of questions. Without further ado, I will turn it over to the witnesses.

Ms. Goulding, go ahead.

[*English*]

Ms. Janet Goulding (Director General, Governance, Policy Coordination and Planning, Department of Industry): Thank you, Chair.

I'd like to introduce my colleagues who are with me today: Bruce Wallace, director of security and privacy policy, and Jill Paterson, a policy analyst with our digital policy branch.

Your committee has chosen to study a very important and timely issue. The protection of personal information online is a prerequisite for a strong global digital economy. I am here today to provide some background on the federal legislation that protects the privacy of Canadians in commercial transactions, online and elsewhere, the Personal Information Protection and Electronic Documents Act or PIPEDA.

[*Translation*]

Since it was implemented, PIPEDA has provided a solid foundation for the protection of privacy online. Canada's federal private sector privacy law is regarded around the world as a model for other countries to follow when seeking ways to protect the privacy of individuals. Much of its strength comes from the manner in which PIPEDA addresses privacy in a technologically neutral way, using a flexible, principle-based approach.

PIPEDA deals with two distinct issues. Part 1 sets out the privacy protection obligations under the act. Parts 2 to 5 deal more with electronic documents than with privacy, and as such are not relevant to your current study.

Part 1 of PIPEDA sets the rules for the private sector in protecting personal information used in the course of business. It establishes clear ground rules that govern the collection, use and disclosure of personal information.

[*English*]

The act balances two central considerations: the need to protect the privacy of individuals, and the need of organizations to collect, use, or disclose personal information in the course of commercial activities. Striking this balance is particularly relevant in the online environment, where large amounts of information can be rapidly collected and stored, and financial transactions can be completed in just a few seconds.

There are some key features of the act I'd like to touch on today.

First, the act applies only to personal information that's used for commercial purposes. It applies to personal information in all formats—electronic and non-electronic. The act applies across the economy as a whole, not just to individual sectors.

Second, the law is based on a set of principles taken from the Canadian Standards Association's Model Code for the Protection of Personal Information. The code was developed by the private sector and consumer representatives and was adopted well before the act came into force. The code is a set of 10 core privacy principles, which were incorporated into schedule 1 of the act.

I'd like to draw your attention to the most central principle, which is the need for consent. Privacy legislation in Canada, and in many other countries, is founded on the principle of consent, whether that be expressed or implied, to collect, use, and disclose personal information.

The act also requires that any collection, use, or disclosure of personal information by an organization should be considered by a reasonable person to be appropriate in the circumstances. This is an overarching test that applies to all provisions of the act. This requirement brings a significant degree of flexibility to the legislation, allowing PIPEDA to remain applicable while social norms, behaviours, and expectations change over time and in different situations, both online and offline.

PIPEDA first came into force in 2001, before the onset of online services and activities—such as Twitter, YouTube, Google, and Facebook—which today we take for granted. Yet as the Internet has evolved, and as new services have been introduced, the legislation has proven to be an effective tool. Its flexibility, resulting from its technology-neutral and principles-based approach, has enabled Canada's Privacy Commissioner to address the challenges that have arisen online, including in social media environments. She has enforced privacy provisions on an international scale against some of the world's largest online service providers, including Google and Facebook.

For example, following an investigation by the commissioner, Facebook took corrective action to bring practices in line with obligations under PIPEDA. Facebook agreed to provide information to help users better understand how their personal information will be used so that they can make more informed decisions about how widely to share that information.

● (1225)

Overall, the legislation continues to provide a robust framework on which to find a balance between business practices and protecting the privacy of Canadians. However, technological innovation, combined with continual changes to individuals' online practices, highlight the importance of reviewing PIPEDA to ensure that it can appropriately address emerging challenges.

[*Translation*]

In particular, the development of applications for individuals to share information about themselves—a key aspect of what is known as "Web 2.0"—is changing online behaviour. Much personal information is volunteered by individuals themselves. And despite being active participants in the flow of personal information, many users may not fully understand the way their information is used, or the associated privacy risks.

Research indicates that social media users may not anticipate how broadly accessible information they post will be. In addition, the use of "cookies" and other online tracking tools is pervasive, and yet largely invisible to the average Internet user. The potential exists for personal information to be aggregated and used in ways which the individual may never have even imagined and with which they may disagree.

[*English*]

There are complex issues involved in the development of policy frameworks to maintain privacy protection in this environment. Canada is one of many jurisdictions currently grappling with this. The OECD, for example, is currently conducting a review of its privacy guidelines, which were the first internationally agreed-upon set of principles and which influenced the development of the CSA model code, upon which PIPEDA is based.

Likewise, a good piece of legislation like PIPEDA can be made even better with regular review to ensure that it keeps pace with advancing technology and evolving business models.

Bill C-12, the Safeguarding Canadians Personal Information Act, will update PIPEDA in a number of important ways. The bill, which is awaiting second reading in the House of Commons, is the result of the first review of the act, which was undertaken by your predecessors on this committee in 2006-2007. At that time the committee concluded that no major changes to the act were needed; however, they did make a number of recommendations aimed at improving some elements, notably the need for mandatory data breach reporting requirements.

Following the committee's report, Industry Canada conducted extensive consultations, leading to the government response, which indicated that several amendments to PIPEDA would be made to address the committee's recommendations. These amendments were first tabled in May 2010, but subsequently died on the order paper. The amendments were later reintroduced as Bill C-12, which was tabled in September of 2011.

Significantly, Bill C-12 will create a powerful tool to protect and empower consumers online. The bill establishes a framework under which businesses must notify customers when their personal information has been lost or stolen. Canada's Privacy Commissioner has long called for a legislative approach to data breach notification. In 2007, her office published voluntary breach notification guidelines, but she has expressed concern that not all businesses are reporting data breaches, nor have all organizations taken appropriate security precautions to protect their holdings of personal information.

Bill C-12 requires organizations to notify individuals in cases where a breach poses a real risk of significant harm, such as identity theft or fraud or damage to reputation. The Privacy Commissioner will also be informed of any material breach, thus allowing her to exercise oversight of compliance with the new requirements. Consistent with her current compliance powers, the Commissioner will be able to publicly name organizations that fail to meet their obligations if she feels this is in the public interest. This is a powerful inducement for organizations to act in good faith. In fact, we have seen this power compel change in the practices of well-known social media companies such as Facebook and Google. Several high-profile data breaches in the past several years, such as those experienced by Sony and the large e-mail marketing firm Epsilon, have underscored the need to pass this bill and its new notification requirements quickly.

The bill also includes enhancements to the consent provisions designed to protect the privacy of minors online. Research shows that children may not have the capacity to understand the consequences of sharing personal information. Not all marketing activity directed at children is inappropriate; however, some online services surreptitiously collect personal information about children in an environment that is often designed to look like playgrounds or educational websites. Therefore, Bill C-12 requires organizations to make a reasonable effort when collecting the personal information of minors to clearly communicate why it is being collected in a way that would be understood by the target audience.

We believe these changes are an important step towards ensuring that our privacy legislation continues to protect Canadians.

Thank you for the opportunity to come before the committee today. My colleagues and I would be happy to take your questions.

● (1230)

[*Translation*]

The Chair: Ms. Goulding, thank you very much for your presentation and for being here.

Ms. Borg now has five minutes for questions.

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

I would also like to thank the witnesses for being here today.

Companies like Facebook and most social networks are not located in Canada, but we know that they have a lot of Canadian users. What is our legislative power over foreign companies that are active within Canada? What influence does our country have internationally?

[*English*]

Ms. Janet Goulding: The legislation applies to information collection in the course of commercial activities here in Canada. But clearly, the activity and the companies collecting that information can be international, so the importance of international cooperation on behalf of the Privacy Commissioner is a key element.

Recently the legislation was updated to allow the Privacy Commissioner to share information more broadly with her international counterparts.

[*Translation*]

Ms. Charmaine Borg: Thank you.

We all know that the Internet develops and changes very quickly. New websites are always being launched. It is growing so quickly that we are always trying to catch up. For me, it was important to have proactive measures to avoid a fear of using the Internet. I think this is all part of a digital strategy that your department announced. We haven't really seen anything new in this respect. So I would like to know if you have anything new to share with us.

[*English*]

Ms. Janet Goulding: In terms of digital policy, certainly the government has been very active. The passage of the recent anti-spam legislation is a key element, along with the amendments to PIPEDA that are currently before the House, in addition to the copyright legislation.

The minister has recently indicated that he will be releasing a strategy later this year. Many elements of the digital economy continue to evolve in Canada, and the government and the private sector continue to respond to those challenges.

[*Translation*]

Ms. Charmaine Borg: Unfortunately, I think we are really lagging behind when it comes to everything Internet-related. I think that a lot of work needs to be done and that it is better to be proactive than wait until there's a disaster.

On that same topic, the commissioner, Ms. Stoddart, said in her testimony, and as you explained in your presentation, that Canada is lagging behind with respect to standards for data breach. Perhaps Bill C-12 doesn't contain enough measures.

Can you please explain why we lag so far behind when it comes to informing users about breaches of their personal information?

● (1235)

[*English*]

Ms. Janet Goulding: I think the commissioner was pointing to the fact that Canada is one of the few remaining countries that do not have mandatory data breach reporting requirements. Therefore, as I indicated, it is important for Canada to catch up and pass the amendments in Bill C-12 that are currently before the House.

In terms of going forward, the commissioner made reference to the overall compliance powers under the act and suggested that the second parliamentary review would be a good opportunity to take a second look at that. Perhaps that's something parliamentarians would like to do.

[*Translation*]

Ms. Charmaine Borg: Do I have any time left, Mr. Chair?

The Chair: You have a minute and a half.

Ms. Charmaine Borg: I've spoken with a number of stakeholders and academics in this area. Ms. Stoddart also gave the example of a company that kept its data because it didn't have the technology to purge the data. So I think we have technology that is being adopted and invented, and the policy comes afterward.

I would like to hear your comments on this as well. How can we make sure—with the policy and then the technology that's developed—how can we make sure that we don't have technologies that will preserve data because we don't know how to purge or destroy it?

[*English*]

Ms. Janet Goulding: In the current legislation, PIPEDA has requirements for organizations to set retention schedules for all of their personal information. The commissioner alluded to that.

In terms of requiring companies to think about privacy as they're implementing new technologies, this is an ongoing challenge. It's something privacy commissioners around the world, and in Canada as well.... The Ontario Information and Privacy Commissioner has been very vocal on her views on privacy by design.

Companies are thinking about how they need to be in line with privacy protection. But clearly, awareness is a challenge. The private sector, as well as individuals, have a role to play in protecting their privacy online.

[*Translation*]

The Chair: Thank you.

Your time is up, Ms. Borg.

Mr. Calkins, you have the floor.

[*English*]

Mr. Blaine Calkins (Wetaskiwin, CPC): Thank you, Mr. Chair. Thank you very much, Ms. Goulding, for being here today.

I have a couple of direct questions for you. They're fairly straightforward and come right out of your testimony.

You said that the OECD is conducting a review of its privacy guidelines. Do you know when that OECD review is slated to be completed?

Ms. Janet Goulding: The review is ongoing, but I'll maybe just turn to my colleague, Jill, in terms of the timelines.

Ms. Jill Paterson (Policy Analyst, Security and Privacy Policy, Digital Policy, Department of Industry): I'm afraid I don't have specific details about that. I know the OECD has recently published some documentation with regard to recommendations for changes to the EU Data Protection Directive. I'm afraid I'll have to get back to you with details on the timing for how they see moving those recommendations forward.

Mr. Blaine Calkins: It would just be helpful for us to know, from a timing perspective.

Ms. Goulding, you spoke a little bit about cookies. Believe it or not, I was a computer programmer before I came here. I taught information technology. I'm fairly familiar with some of the issues that concern this. Everybody who is a computer or technology user should know that there are operating system settings that can be used to set things like security, for example. When it comes to cookies, you can actually turn the setting off so that cookies can't be stored on your computer, and so on.

Do we have an education problem in Canada insofar as people's ability to actually understand what their systems are capable of? I was going to ask this of the Privacy Commissioner, because if you know what you are doing, you can actually set it up in such a way that you can increase your own personal protection of your information.

Are we doing enough on that front in Canada to make sure people are fully aware of the risks they face, and what some of the things are that can help mitigate these concerns?

Ms. Janet Goulding: Thank you for the question. I do think you raise a very important point. Digital literacy has been an issue that has been raised over and over again in the context of having people understand what their privacy risks are online. I do think digital literacy needs to be a priority. Awareness is an important element. It's important, as the commissioner pointed out, because schoolchildren are coming online sooner and sooner. For them to understand the potential risks they face when they put their information online is key.

Again, I mentioned to you briefly that one of the amendments in Bill C-12 will impose a new obligation, or a clearer obligation, on organizations to target their messaging at their target audience. When you're talking about children, or frankly, the average Internet user, it's important they're aware that there are measures they can take to further protect their privacy online.

● (1240)

Mr. Blaine Calkins: I have something that I hope for some clarification on. In one of your first paragraphs, you say the act balances two simple considerations—the need to protect privacy of individuals, and the need for organizations to collect user-disclosed personal information in the course of commercial activities.

I think everybody understands that a financial transaction—for example, every time you use a Visa, debit card, or do an online banking transaction—certainly is a commercial activity, but is signing up or downloading an app off of iTunes that's free....? Do we actually need money to change hands in order for this to be considered a commercial activity? Is signing up for a free e-mail account on Gmail considered a commercial activity? Or is the commercial activity actually when somebody takes the personal information that you volunteered as, I would guess, the fee for the free service, and then resells that information?

I'm sure everybody who is watching this would clearly know that sometimes within minutes of signing up for a free app or whatever, as soon as you give your e-mail address, all of a sudden your inbox is full of spam. Sometimes it takes less than a couple of hours for that to happen. So you know that your information that you have just submitted has been either divulged, sold, or whatever the case might be.

What protections do I have when I sign up to know that my personal information has been sold? Do I have to read those 15 pages of jargon, or is there something a little more clear that Canadians can grapple with?

Ms. Janet Goulding: Thank you. I think the question of clarity is an important one. You're absolutely right in terms of the need for clarity when organizations are seeking to collect information that they will use for a commercial activity. I think it's clear that an actual transaction....

It might be arguable that when downloading a free app, there is still a transaction going on there. But clearly, information is collected in a commercial context in many ways, whether or not money is actually changing hands. Clarity about what that information is being collected for and how it is being used is a real challenge in today's environment.

[*Translation*]

The Chair: You only have a few seconds left.

[*English*]

Mr. Blaine Calkins: From my perspective, then, do you think it would be feasible to implement a system whereby Canadians would be notified any time their personal information was sold or shared in a commercial way?

Ms. Janet Goulding: The challenges that are presented in the online environment can make that difficult. The Privacy Commissioner alluded to that simply in that, although the information may be contained, you have to get through a 10-page terms and conditions statement to actually find that information. All too often, Canadians or consumers just click "accept" and move on to the next phase of their transaction.

So getting back to your first question, digital literacy is key, and people need to take an active role in protecting their own privacy. I don't know that I have a more precise answer to your question.

[*Translation*]

The Chair: Thank you.

Mr. Andrews now.

[*English*]

Mr. Scott Andrews: Thank you, Mr. Chair, and welcome.

To continue on that concept, the first thing, the most central principle you said is the need for consent. When you're talking about consent, how much jargon can be in there? How simple can we make it? I know we talked about the Privacy Commissioner, when someone has consent—you give consent to give your information to somebody else—how simple can we make this, so that people get it, and everyone knows what we're doing when we give consent? Is it possible?

Ms. Janet Goulding: I would have to agree with the Privacy Commissioner on this front. I think it is possible, but it is up to organizations to make those clear statements to their users as to what they're consenting to and what their information will be used for.

Mr. Scott Andrews: You also said that this is whether consent is "expressed or implied". Can you give us an example of implied consent? Should users be very concerned that some of this may be implied and they don't realize it?

Ms. Janet Goulding: The legislation indicates that implied consent depends on the context and the circumstances around it. So, for example, if the consumer is purchasing a magazine subscription, their consent might be implied to get a follow-up notice about the fact that their subscription is expiring, but it's very much contextual and it depends on the circumstances in place. So that kind of framework allows flexibility in allowing the Privacy Commissioner to interpret what's reasonable in the context of implied consent. I think it's one of the valuable aspects of the legislation.

Once you move to something that's more prescriptive, then by definition you tend to exclude something you can't foresee, and so the principles are very flexible and that's one of the strengths of the legislation. But the Privacy Commissioner has issued a number of guidelines on how consent should be interpreted, and they are available on our website.

● (1245)

Mr. Scott Andrews: Quite often now, you see when you sign up that there's a box to be ticked beside a sentence that says, "We will provide this information to other vendors" and you can tick it if you wish to do that.

If you do tick the box, how far does it go down the chain to these vendors or other groups? How about the resale of this data? Does that go on? Does some organization get this data from somewhere else and then in turn resell it to somebody else? Are we concerned that this data gets passed through many hands through the resale?

Ms. Janet Goulding: I can't speak to all business models but I don't think what you're describing is unheard of. I think that the principle of consent applies, no matter what the context. So if the information that's being collected is to be passed on to a third party, that consent is required by the legislation to be explicit and informed.

Mr. Scott Andrews: And even if that third party then resells it?

Ms. Janet Goulding: Certainly within the context of the legislation, I would say, yes.

Mr. Scott Andrews: Talking about breach notifications, the Privacy Commissioner said that not all businesses are reporting data breaches. How widespread do you think data breaches are?

Ms. Janet Goulding: Unfortunately, we don't have any research available to us to indicate how widespread data breaches are, but I think that in a world where organizations have vast amounts of data at their fingertips, it's important that we have legislation that requires all organizations to be subject to the same level playing field, and that they be required to take measures to protect that information in a manner consistent with the sensitivity of the information.

I think once the legislation is in force, the Privacy Commissioner will have the ability to have a better understanding of how widespread data breaches are in Canada.

Mr. Scott Andrews: How quickly would notifications of these breaches need to be divulged to individuals?

Ms. Janet Goulding: Again, the speed with which the notification needs to happen is commensurate with the potential harm. If there's a significant risk of harm, you would expect that this notification should take place very quickly so that people can act to protect the information that may have been breached.

So for instance, in the example of potential credit card breaches, individuals might want to act quickly to cancel cards or further protect themselves. Again, the legislation is not prescriptive but it does say, "as soon as feasible".

[*Translation*]

The Chair: Mr. Carmichael has the last five minutes.

[*English*]

Mr. John Carmichael (Don Valley West, CPC): Thank you, Mr. Chair, and welcome to our witnesses today.

I'd like to follow up on my colleague's questioning regarding the data breaches. I understand there is an amendment that would safeguard consumers against data breaches.

The concern I have is that the Commissioner was talking earlier about the fact that she lacks the enforcement ability on some of these challenges, so we put in the data breaches. We've covered that off in the legislation, but I wonder what the penalties are. How do we protect consumers? Even though you have it in there, who's responsible to lock that down?

Ms. Janet Goulding: Under the legislation, the Privacy Commissioner is responsible for enforcement of complaints. She does have the ability to launch an investigation, to make public her recommendations, and if she feels further action is required, to take that matter to the Federal Court. The Federal Court can order organizations to change their behaviour, and it can also award damages. The current legislative regime is based on an ombudsman approach, but as the commissioner alluded, perhaps in the second parliamentary review of PIPEDA, the issue of her compliance powers might be something that parliamentarians want to study.

● (1250)

Mr. John Carmichael: With the amendments to the legislation, I understand we now have some protection built in for children and vulnerable individuals. I watched a three-year-old grandson navigate an iPad with remarkable ease. Certainly he didn't read all the governing bylaws getting into what his responsibilities are.

Then I think of seniors on the other end of the scale. Having run numerous anti-fraud seminars in my riding, I've heard countless stories of fraudulent activity involving seniors on Internet sites or being directed at them through their e-mails, and all kinds of different challenges to their security. I have a real concern about how technology is moving at a pace that's faster than we can be in providing security and protection for the consumers using those products. Would you agree with that?

Ms. Janet Goulding: I think the question gets back to digital literacy, and I would agree that it's very hard for consumers to sift through the plethora of information that's probably available on various Internet applications. I think the issue of digital literacy is one that will come back over and over again. Placing requirements on organizations to communicate in a way that is clear and understandable to the target audience is key, and again, something that we hope to see brought into force with the passage of Bill C-12.

Mr. John Carmichael: It would be simplified so that we could all understand it.

Ms. Janet Goulding: Yes.

Mr. John Carmichael: How much more time, do I have, Chair?

[*Translation*]

The Chair: You have a minute and three quarters left.

[*English*]

Mr. John Carmichael: I like the concept of the third-party audit of corporations, but I'm very concerned that there seems to be quite a time lag between when the audit is completed and when we can see the results and the corrective action.

Again, back to the security, the management, the accountability, and governance—where do you see your role in that as far as speeding up the process so that we can stay on top of those who have serious breaches and maintain the governance so that our consumers are truly protected?

Ms. Janet Goulding: The responsibility for enforcement of the legislation rests with the Privacy Commissioner, and the concept of having a third-party audit, which I think is a very good one, is something she has brought into play. I think the Privacy Commissioner is best placed to answer that kind of question.

Mr. John Carmichael: I like the concept of third-party audits. She gave us an example, though, of one already being late, and her having, it seems, very little scope to do much about it. That's a concern to me.

That's it. Thank you.

[*Translation*]

The Chair: Thank you, Mr. Carmichael.

The period for questions is now over. I would like to thank the witnesses for appearing before the committee today.

As planned, we are going to spend the last few minutes on committee business.

First, as you've just been informed, there was a mistake in the lobbying report. Since it has already been tabled in the House of Commons, we will have to use a special procedure to correct it. Could the committee researcher please explain the mistake in question? I will then describe what we need to do to correct it.

Mr. Maxime-Olivier Thibodeau (Committee Researcher): Thank you, Mr. Chair.

A mistake was made in the report, in the part that lists the lobbying commissioner's recommendations that the committee accepted. One number is there that should not be. It has no impact on the rest of the report, but the fact that this number is there indicates that the committee retained a certain recommendation from the commissioner that, in fact, it did not, which is why it needs to be corrected.

The Chair: Thank you.

Since the report has already been tabled, what we need to do to correct the mistake is to seek the unanimous consent of the House. So it is a little difficult to make changes without going before the House a second time. It's a fairly simple change, but the mistake could still have certain repercussions, given that it indicates that we adopted a recommendation, when that is not the case. It will be done in the next few days, but we don't yet know when. Regardless, we will need the cooperation of all the parties.

Does anyone have any questions?

Mr. Del Mastro?

● (1255)

[*English*]

Mr. Dean Del Mastro: Thank you, Mr. Chairman.

I note that we're now into committee business. As is customary for the committee, I just request that the committee move in camera for committee business.

[*Translation*]

The Chair: The motion is not debatable. We are requesting a recorded division. It is moved that the committee now go in camera to discuss committee business.

(Motion agreed to: yeas 7; nays 4)

The Chair: Therefore, we are going to suspend the meeting for one minute to give everyone time to leave.

[*Proceedings continue in camera*]

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

SPEAKER'S PERMISSION

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

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

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

PERMISSION DU PRÉSIDENT

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

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