HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 044 • 1st SESSION • 41st PARLIAMENT

EVIDENCE

Thursday, June 7, 2012

Chair

Mr. Pierre-Luc Dusseault

Standing Committee on Access to Information, Privacy and Ethics

Thursday, June 7, 2012

● (1135)

[*Translation*]

The Chair (Mr. Pierre-Luc Dusseault (Sherbrooke, NDP)): We will now begin the meeting.

I want to thank the witnesses we will be hearing from today via videoconference. There will be a 10-minute presentation by the Information and Privacy Commissioner of Ontario and another 10-minute presentation by the Information and Privacy Commissioner of British Columbia.

As we have much less time today, I will immediately hand the floor over to Ms. Denham.

[*English*]

Ms. Elizabeth Denham (Commissioner, Office of the Information and Privacy Commissioner of British Columbia): Mr. Chair and honourable members, thank you very much for the opportunity to speak to you today.

With me today are Caitlin Lemiski and Helen Morrison, senior policy analysts with my office.

I first appeared before this committee in my previous role as assistant privacy commissioner of Canada. Also in February of this year, I appeared before you in my capacity as registrar of lobbyists for British Columbia.

As assistant privacy commissioner of Canada, I led the first investigation by a data protection authority of a social media platform. As information and privacy commissioner for British Columbia, I conducted the first investigation in Canada of the use of a social media site by a political party. Following that investigation, we issued guidelines on social media background checks.

Today I would like to provide you with an overview of British Columbia's privacy oversight model, followed by a review of some of our recent work related to social media. I will then offer my views on the ways in which Canada's privacy laws are meeting the challenges posed by social media and how governments could strengthen enforcement of our laws.

In terms of regulating the private sector, the Office of the Information and Privacy Commissioner monitors and enforces B.C.'s Personal Information Protection Act, known as PIPA. PIPA determines how organizations may collect, use, or disclose personal information. We share the regulatory space with the federal privacy commissioner because B.C.'s PIPA has been declared substantially similar to PIPEDA. PIPA has wide application, though, including coverage of non-profits. It also applies to employee personal information.

PIPA provides the commissioner with order-making powers. For example, I can order an organization to stop collecting, using, or disclosing personal information. I can also require an organization to destroy personal data collected in contravention of the law. In my experience, order-making power provides me with the authority necessary to ensure that businesses are meeting their statutory obligations.

The purpose of PIPA is to govern the personal information practices of businesses and organizations in a manner that recognizes both the privacy rights of individuals and the need of organizations to collect and use personal data for reasonable purposes. Recognizing this balanced approach, privacy laws do not and should not prevent organizations from developing and using technologies that benefit our digital economy.

I fully appreciate the innovation and value of social media. It allows human expression to manifest in new and exciting ways, and it facilitates public participation. Social media also allows people to connect with family and friends, to follow the latest news, and to build online communities.

That said, I share the privacy commissioner of Canada's concerns that social media companies may not be giving Canada's privacy laws enough attention. All organizations, including social media companies, must follow the rules around knowledge and consent and limiting collection, use, and retention of personal data. These rules are particularly significant given the speed with which information on social networks can move and replicate.

I also acknowledge that the international context in which these companies operate can be a complicating factor. Canada has a very different statutory framework for privacy than in the United States where most of the world's most popular sites are based. However, this does not absolve social media companies from complying with Canada's privacy laws. All organizations doing business within our borders are accountable for their personal information management practices. They must follow the law.

Some of the recent investigative work undertaken by Canadian commissioners demonstrates that Canada is able to address some concerns with social media and privacy. However, it's an uphill battle.

● (1140)

In British Columbia, my office recently investigated the collection of Facebook passwords and profile information by a political party that used this information to vet potential leadership candidates. What we found was that although the political party obtained consent from the leadership candidates, the collection of passwords and profile information contravened the act. Under PIPA, an organization may collect personal information only for the purposes a reasonable person would consider appropriate in the circumstances.

We also found that in viewing the candidates' social media profiles, the political party collected information about the candidates' friends and the friends of friends, without their knowledge or consent. As a result of our investigation, the party agreed to stop collecting passwords and adopted the guidelines issued by our office on social media background checks.

In another investigation, we examined the Insurance Corporation of British Columbia's offer to the Vancouver Police Department of the use of its facial recognition database to identify possible suspects from the 2011 Stanley Cup riot. The relationship between social media companies and facial recognition technology is very significant, as many of these companies integrate this technology into their services. For example, last year, Facebook integrated facial recognition into its photo services, allowing for the automatic tagging of persons in uploaded photos. Facebook chose not to roll out this functionality for its Canadian users.

Indeed, ICBC's offer to the Vancouver police highlighted our awareness of the power of facial recognition technology and how attractive it may be for law enforcement. Law enforcement's use of social media is a particular concern, because social media companies possess some of the largest corporate collections of photographs of individuals.

There are important questions about whether individuals actually provide meaningful informed consent for the collection of their biometric information for facial recognition. If social media companies collect this information without proper authority, then any subsequent use of that information by law enforcement may not be authorized. Moreover, tests have called into question the reliability of this technology. For example, at one U.S. airport, a facial recognition pilot project correctly identified volunteers only 61% of the time. Based on this low success rate, the airport abandoned plans to use facial recognition. Yet, those issues remain, because technology will improve, and law enforcement will want to use it. The relationship between law enforcement and social media, particularly in relation to facial recognition software, is an area that would benefit from greater attention and study.

Statutory requirements, regardless of their content, can have little effect unless organizations actually follow them. In my view, the greatest challenge to privacy and social media is a lack of awareness among businesses of their obligation to limit the type of personal information they collect. For example, in British Columbia, many organizations do not understand, and are surprised to learn, that PIPA does not allow them to collect personal information just because it may be publicly available on the web.

In the context of pre-employment screening, an organization's casual approach to collecting personal information online can lead to unsettling results. For example, although it would normally be inappropriate and illegal for an employer to collect information about a prospective employee's age, sexual orientation, or the fact that they may or may not have children, an employer may learn these details by accessing a social media profile. Personal information on these sites is prone to inaccuracies. In addition, like a dragnet, organizations may catch far more than they intended when collecting personal information from these websites.

Some say that individuals just have to take responsibility for what they post online. While it is true that we should think before we post, this doesn't mean that we should refrain from reasonable opportunities to express ourselves. In the end, it's all about context, and Canada's privacy laws recognize this by limiting collection and use to what is reasonable in the circumstances.

As Canadians' views about communication and expression evolve, the challenge for commissioners and governments is to help organizations understand these new distinctions. Mothers should not refrain from posting information about their parenting experiences for fear of repercussions from their employers, and friends should be free to make comments about products and services to each other without unreasonable market surveillance and profiling.

These observations are consistent with a 2010 report by the Office of the Privacy Commissioner of Canada, which states that "traditional notions of public and private spaces are changing. Canadians continue to consider privacy to be important, but they also want to engage in the online world." Sustained public education and engagement will be necessary to promote awareness and compliance with Canada's privacy laws in the world of social media.

In conclusion, social media companies should use the innovations that make them so popular to uphold the values of privacy that are important to Canadians. Protecting privacy is about more than obtaining an individual's informed consent. It is about what is appropriate in the circumstances.

Although principle-based, technology-neutral laws adapt to new technology, in my view, strong enforcement tools, such as order-making power and mandatory breach reporting, are critical for the federal privacy commissioner to regulate the space.

Thank you very much for the opportunity to appear before you today. I'd be pleased to respond to any questions.

● (1145)

[*Translation*]

The Chair: Thank you.

Without further ado, I will give the floor to Ms. Cavoukian, who will be speaking with us from Toronto and whose speech will be 10 minutes long.

[*English*]

Dr. Ann Cavoukian (Commissioner, Office of the Information and Privacy Commissioner of Ontario): Good morning, ladies and gentlemen. My thanks to the chair and members of the committee for inviting me to speak to you today.

I'm not going to speak to you about privacy regulatory matters and existing statutes. The reason for that is you've heard from Commissioner Stoddart on that subject. You've heard from legal scholars like Michael Geist. You've just heard from Commissioner Denham. There's very important work that needs to be done in the regulatory and legislative space.

The reason I'm not talking to you about that today is not because I do not have strong regulation in my own jurisdiction; I have order-making power, and I cannot emphasize enough how important order-making power is to a regulator. I also have, under PHIPA, the Personal Health Information Protection Act, a wonderful ability in terms of mandatory breach notification. We have these tools at our disposal, and they're excellent, but I'm not going to be talking to you about that today.

I'm going to talk to you about the future of privacy. I'm going to take the next 10 minutes to talk to you about something called privacy by design. Before I start that, though, please allow me to introduce my colleagues. I'm joined by Michelle Chibba, my director of policy, and David Goodis, my director of legal services.

Privacy by design is all about ensuring that the user has control of their data. Increasingly what we are experiencing all around the world is that with the enormous growth of mobile technologies, wireless WiFi everywhere, online social media, mobile devices, with the growth of information sharing and availability, it is becoming extremely difficult to regulate this information strictly after the fact —meaning you allow the privacy harm to arise, someone complains, we investigate, and then we offer a system of redress. That's very valuable and must continue, but using those tools, we only catch, in my view, the tip of the iceberg in terms of the potential pool of privacy infractions and privacy-invasive activities. Privacy by design is all about being proactive and trying to prevent the privacy harm from arising to begin with.

You'll see that privacy by design was adopted as an international standard two years ago in Jerusalem by the international community of privacy commissioners and data protection authorities. It was unanimously passed as an international standard and has since then been actually reflected in work coming out of both the United States and the EU. The FTC in the United States, the Federal Trade Commission, has just in January of this year put out its piece on how it sees privacy moving forward in terms of regulatory structures and private sector self-regulation. They've recommended three practices. The first of those three practices is following privacy by design.

If you look at the regulation put out by the EU on data protection earlier this year, you'll see the language of privacy by design, and privacy as the default permeates the entire regulation. You may be interested to know that privacy by design has now been translated into 25 languages. I assure you this is no small feat. It is reflected in all of the major languages around the world. I just want to give you an idea of the import of privacy by design and how seriously it's being taken all around the world.

Now I'm going to walk through, very quickly, the seven foundational principles of privacy by design. Let me try to summarize this for you. The essence of privacy by design is to embed privacy into the design of not only information technologies but accountable business practices, policies, and procedures in a proactive way, in an effort to prevent the privacy harm from arising as opposed to reactively offering a system of redress after the fact.

● (1150)

The essence of privacy by design is being embedded as what we call the default setting. By that I mean that when privacy is the default condition, you, as the user, the data subject, can be assured of privacy. You don't have to look for the privacy. It's guaranteed. It's automatic. It's embedded in the system as the default setting. That is key, and that is an integral part of privacy by design.

The other essential feature is that it talks about operating in a positive-sum, not a zero-sum, environment. Zero-sum means that you can have one or the other of two interests. You can have privacy versus security, privacy versus social media, or privacy versus biometrics. Get rid of the versus.

Positive-sum means privacy and other functionalities. You have to have privacy functioning in an environment in which it can operate in unison with other interests, as it must. The future is all about creativity and innovation. Who knows what's around the corner in terms of the next technology and the next development? We welcome that. We insist upon privacy being part of the package.

You've all heard a great deal about big data. I'm not going to talk to you about that today, because there is no time. Just for your information, here's a little teaser. Tomorrow we're launching a paper we did jointly with IBM called “Privacy by Design in the Age of Big Data”. We're releasing this tomorrow morning at conferences in Washington, D.C., and Toronto. If you look at our website tomorrow, please take a look at our paper on how you can have privacy and big data.

I'm going to talk to you for the remaining four minutes I have about an example of how privacy by design actually works on the ground. I don't want you to think this is simply a theoretical formulation or some academic construct. It's real. It's operating right now on the ground.

Let me tie this to Facebook and other social media. As Commissioner Denham mentioned, Facebook has the capability of facial recognition technology. So photographs that are uploaded to Facebook can be tagged with an identity through facial recognition technology. You can imagine what a treasure trove this will be for law enforcement and other interests, with the pictures, the faces, of 900 million users, potentially, being tagged, using facial recognition technology, and potentially matched with pictures of faces taken from a crime scene, for example. The police would come knocking on the door of Facebook with a warrant. Of course, Facebook would have to give them the information.

I'm going to tell you about a technology we've introduced here in Ontario that would not allow that to happen, even though it would allow facial recognition technology to happen. It is facial recognition technology using privacy by design biometric encryption.

Let me just tell you very briefly what this is. In Ontario, the OLG, the Ontario Lottery and Gaming Corporation, is the corporation that runs our casinos in this province. We have 27 casinos in Ontario. They're run by the OLG.

They came to me a few years ago and said that they had a problem. They have an addicted gamblers program, a problem gamblers program, called the self-exclusion program. Quite simply, if you are an addicted gambler, and you're going through the equivalent of a 12-step program, such as Gamblers Anonymous, and you go through the entire program, the last thing they'll ask you to do is go to the casino of your choice and ask to be placed on the self-exclusion program. That means that you want to give up gambling, have gone through the whole program, but know that you might fall off the wagon and try to go back into that casino and gamble, and you don't want to do that.

The self-exclusion program is completely opt-in. It's voluntary. You go to the casino of your choice and you say, “Sign me up. I want you to keep me out. If you see me trying to enter your premises, I'd like you to ask me to leave, please.” You fill out the form. They take your picture. You sign it, and this is completely your choice.

The problem was that this program wasn't working very well. In the past, the form you filled out with your picture on it and all that would live in some back office somewhere in a file cabinet.

● (1155)

In the meantime, these addicted gamblers who fell off the wagon would try to sneak back into a casino. They would go to the front of the casino—there are 27 of them across the province—and they would sneak back in. They were very good at it and they would successfully get back in. Unfortunately, many of them would lose their life savings. They would lose their families. They would lose their jobs. It was terrible. Then they would sue the Ontario government—the casino—for not honouring this program and keeping them out. It was a lose-lose.

So when the OLG, the Ontario Lottery and Gaming Corporation, came to us and asked for a solution, they said, “Here's what we can do”. They said they had cameras at the front of all casinos. Casinos all around the world have cameras at the front for security purposes. They said that if they were to match the cameras at the front with the faces in their backroom files, then they could identify these self-excluded gamblers and keep them out.

Here's the problem with that—facial recognition technology can pick up the faces of a lot of people entering the casino, not just the problem gamblers. Plus, this could then be made available to others for secondary uses like law enforcement. I wanted to ensure that wouldn't happen.

So what we did was that we asked them to use a program called biometric encryption. What this means, very simply, is that this is a system of using a facial recognition data capture in a way such that it cannot be used for any other purposes. When you use biometric encryption, no biometric template—as it is called, which is a digital representation of the face or the finger—is retained in the database.

Quite simply, all that means is that if law enforcement comes knocking on the door and wants to access your database of biometric templates to see if there's a match to a crime scene, you can't give them the biometric template because it doesn't exist. The only use that can be made of this information is for this particular purpose, the primary purpose which is intended.

I can explain to you later, if we have time in questions, how this works. But this has been tested in other jurisdictions. In the Netherlands, priv-ID, another company, has done this, and I can give you other examples.

This is a wonderful, privacy-protected biometric solution that allows the particular privacy biometric problem to be addressed, but doesn't allow the information to be used for any other purpose.

● (1200)

[*Translation*]

The Chair: Pardon me, but I must inform you that you have approximately one minute left to conclude your presentation.

[*English*]

Dr. Ann Cavoukian: I'm going to ask you to consider privacy by design as a solution on a go-forward basis in terms of how we protect privacy. For example, if we ask Google, Facebook, and others to implement privacy by design solutions such as biometric encryption for their facial recognition program, we will have far greater privacy, as well as the functionality that was intended by the social media in that particular program.

You can have both privacy and other core functionalities operating in unison, but I urge you not to allow one at the expense of privacy.

Thank you very much, ladies and gentlemen.

[*Translation*]

The Chair: Thank you.

I now hand the floor over to Mr. Angus, who will have seven minutes.

[*English*]

Mr. Charlie Angus (Timmins—James Bay, NDP): Thank you very much.

I want to say at the outset, Madam Denham and Madam Cavoukian, congratulations for your leadership on the issue of protecting the privacy rights of Canadians. You both have been champions of the issue and have been very forward-thinking. It has been very helpful.

I'm interested in the issue of privacy by design because the problem with legislating a solution is that, if we are simply looking at going after the problems after the fact, we're always playing catch-up and that's not a system that I think is conducive to building the kind of social media world that we're interested in.

So the question of privacy by design I think is fascinating and is one that I hope our committee seriously studies. I compare it to the issues in the 1990s across Canada with the forestry industry and the fights with environmental groups. It seemed that there was continual conflict until the sides sat down and started to come forward with a standard, which was forestry certification—the FSC. There are still a lot of problems with the FSC, but it became a standard that people had to meet in order to find a way to get past the continual conflicts in the forest.

It seems to me that this might be a way of moving forward on issues of privacy. My question is, does it have to be legislated? Do we have to just hope for opt-in from the giants and from the small players? Or is there a way of saying that when you're dealing in Canada this needs to be set up, that this is the gold standard and we expect you to stand by that gold standard? How do we actually make this doable on the ground?

Dr. Ann Cavoukian: Thank you very much for that question.

I think there's one way that we can do it. I'll refer you to a paper that we released this past summer—I'm trying to remember the name of it—"Privacy by Design in Law, Policy and Practice". The idea for the paper came from Commissioner Pamela Jones Harbour, who is a former commissioner with the Federal Trade Commission. When she was talking to me about privacy by design, she said we could impose it as a requirement, a condition, in our consent decrees, in decisions that the FTC issues upon completion of an investigation, and we could include it as something on a go-forward basis that a company would have to follow proactively from that point on.

Justice La Forest kindly reviewed the paper that I just mentioned, which you can find on our website, and he said that privacy by design is an excellent idea that should be incorporated into administrative means of law addressing privacy on a go-forward basis.

One way we could do it—I know that Bill C-12 is looking at changes to PIPEDA—would be to have some way of saying that on a go-forward basis, at the conclusion of an investigation, a company would be required to follow privacy by design in any particular area that was problematic.

The other thing about privacy by design is that it's not a punishment. We always say privacy is good for business. There should be a privacy payoff to businesses that follow good privacy practices. Consumer confidence and trust are being eroded very quickly in this day and age, and you can strengthen that on the part of your customers. It is not something that is in fact a stick. It is both a carrot and an inducement to introduce privacy protections in a way that ultimately will save the company resources, because they'll be able to avoid privacy infractions and privacy investigations, and potentially, class-action lawsuits that are coming out.

There's so much happening on the privacy front that when we talk to companies about privacy by design we do it because they invite us to tell them how to do it. They want to do it, not only for the right reasons but for business-related benefits as well.

I think there is a way forward by imbedding it into new regulatory structures.

● (1205)

Mr. Charlie Angus: Thank you for that. I think that's an interesting way to look at the issue.

I don't think our experience has been that the companies that are out there developing social media are looking just to grab data and then make off with it. It's the unintended consequences, the stalker's paradise.

Dr. Ann Cavoukian: Yes.

Mr. Charlie Angus: Young people put all manner of pictures on Facebook and everything is tagged. If someone decides they want to harass or follow someone or make their life a living hell, the technology becomes very simple, and there are unintended consequences that nobody necessarily thinks about when they set this up. If we embed it into the operating system, people don't have to worry about that happening.

Are we looking to have a few of the big players come forward and proactively do this? You're saying there's a lot of international support. How do we really make it operational?

Dr. Ann Cavoukian: Mr. Angus, I love that you refer to "unintended consequences". I didn't use the slide here, but I have a big slide when I talk to, especially, tech companies. My slide just reads: beware of unintended consequences. That is always the fear.

I called last year the year of the engineer, because I talked to engineers at all of the leading companies around the world. I talked to Adobe. I talked to Intel, and HP, to Google. I've talked to Facebook and others, but I specifically wanted to talk to their engineering, computer science technical teams to translate, if you will, or operationalize the principles of privacy by design into code.

Of course, we've been talking to lawyers for years, so I'm not worried about lawyers and policy writers understanding how to translate the policy requirements into policy codes, etc., but the engineers were being left out and the computer scientists. When I talked to them, I said, this is very simple. I can't write the code for you, but I can translate this into what does "primary purpose" mean, and how do you ensure that data minimization principles are being reflected in your operational procedures.

Privacy as the default is such a critical feature. We try to explain this not only to engineers—and they get it, of course—but to laypeople. I always have what I call my neighbours' test. I have very clever, smart neighbours, but they're not in the privacy field. So I try to explain it to my neighbours, and if they grasp the concept, which they will, then we're off and running. It has to be accessible to the public and to engineers alike, and the notion of privacy as the default resonates. As one of my neighbours said, does this mean I get it for free? I don't have to ask for it? I don't have to scour the privacy policy to find it? I just get privacy for free? I said, yes, it would be embedded in the system by default as an automatic feature. She said, "Sign me up. That's what I want."

That's the kind of discussion we have. As I said, we talked to all of the major companies. For Google+, when they were doing their beta test for Google+, their new online social media, we participated in the beta. They're very interested in the privacy issues. They've come up with this concept of circles and restricting privacy and sharing within a given circle. So you could have one for your workplace colleagues, one for your neighbours, one for your family, etc.

We've talked to all of the major companies about privacy by design, and I would hazard a guess that if you went to any of them they would know about it.

● (1210)

[*Translation*]

The Chair: Thank you.

Your speaking time is unfortunately up, Mr. Angus. As you know, the seven-minute period includes questions and answers.

I now give the floor to Mr. Calkins, who will have seven minutes.

[*English*]

Mr. Blaine Calkins (Wetaskiwin, CPC): Thank you, Mr. Chair, and thank you to our witnesses today.

It's great to have two provincial commissioners here. There's certainly a lot of experience in your presentations.

I'm going to come at this from the perspective of one of those computer programmers who dealt and struggled with some of these issues in a life prior to becoming a member of Parliament.

Mr. Michael Geist was before our committee here a few days ago —and I think Mr. Angus was going down this road—but I'm deeply concerned, not only as a personal consumer and person who's making his way through the Internet these days but because I have young children at home whose situation I'm worried about. Of course, as a parliamentarian, I'm always worried about issues pertaining to the privacy of my constituents and so on. So this is quite a timely and interesting study that we're doing right now.

I agree wholeheartedly with the premise that defaults.... Mr. Geist's comments were that the "devil is in the defaults". It would seem to me that some of the default settings that we have, whether they're at the operating system level, whether they're at the browser level or the interface level, whether they're at the data level, are somewhat concerning. I would just like to give both witnesses an opportunity to talk about that a little bit more.

I certainly do agree that—in your privacy by design presentation, item 2, "Privacy as the *Default* Setting"—is something that I think most Canadians, if they were given an opportunity to have this reasonably explained to them, would enjoy.

I also believe fully that I should be explicitly asked, as a consumer, if any of my personal information should be collected. It should not be written up in some 15-page legal document, where unwittingly, with the press of one little button, I must accept the entirety of a document. I have no ability to parse out and accept those parts that I do agree with and those parts that I disagree with, I must accept the entirety of signing on to an account, or whatever the case might be, in order to partake in whatever transaction that I'm doing.

I just wonder if there are some practices out there or some recommendations you have that would help consumers navigate through this ever-increasingly complicated web.

Ms. Elizabeth Denham: I think consent is very significant in the online world, but it's only part of the answer. I also agree with you that end user agreements, with the lengthy notices and the legalese is not the solution to the problem. Some very good work has been done in short, just-in-time notices. That's even more important in the mobile environment because you certainly can't read consent and user agreements at the end of the day.

Our laws in Canada are flexible. They require the collection of the data to be reasonable, and there needs to be transparency. In an ecosystem as complex as a social media site, it is difficult because I think consumers don't understand what is behind the curtain. They don't understand all the groups they are communicating with, how the data is flowing, and how third parties are using their information. It's a brand new environment.

Historically, we have dealt with a consumer doing business with one brick and mortar company. It is very clear whom you are doing business with. Consent works quite well in that environment. I think what is needed here is a much more sophisticated approach.

I think it starts with accountability. Our office, in conjunction with the Alberta and the federal office, has just issued guidance on accountable data governance, what privacy looks like on a comprehensive level. That's where we go down the road. We look at the company overall to make sure their practices, policies, and control, such as privacy by design, are dealt with in a comprehensive way across the board.

● (1215)

Mr. Blaine Calkins: Thank you.

Dr. Cavoukian, do you want to add anything to that?

Dr. Ann Cavoukian: For starters, users, consumers, and all of us have to be more vigilant, and we have to speak up with the companies that we do business with. You may say that's hard to do. Facebook is the way it is. How are you going to get changes? You would be surprised at the number of times they have changed. When they introduced a privacy practice, like their news feed in 2006, everyone blew up at that, and then they reversed it. There have been a number of missteps, and it's only because the public has spoken out that they have pulled back.

Let's talk for a moment about what companies can do and what we can ask businesses to do and governments as well. Mobile devices, as you know, are the way of the future. Everyone is going into mobile. You can't read anything on that in terms of the policy and other things. For example, in the United States people are using a blue button. I think the blue button was made available for veterans in the U.S. to access their health data. What did Veterans Affairs have on them? They had this blue button, and they would immediately see what they had on them. The same idea is coming out for a green button for the energy sector. If you want to see how much energy you've used, people have said there should be a green button. You'd press it, and you would see how much energy you are using, and you can compare it to others like your neighbours, etc.

What this speaks to is not only companies being far more careful but circumspect about the information they automatically collect from consumers without their knowledge or consent. The opposite of privacy as the default is public as the default. We have to reverse that. We have to change that. Also, they have to know they have to be accountable to you, the user, the data subject. They have to be transparent with the information they have about you in their possession, in their databases. You should know what they have. Unless you know what they have in their possession, you won't know what's at risk, and what might be, if it's hacked, or if there is a data breach.

LinkedIn was just hacked and their passwords accessed. You are not going to know what they're going to have access to. It's very important to have that kind of transparency. Then, all of us speaking up and getting on the case of business. Don't misunderstand me, I'm not anti-business at all. I love business. We have to have strong businesses to have a strong economy. They also need to know they have to protect their customers and their customers' information. How can they do that? We can help them figure out how to do that and be transparent with their customers.

Mr. Blaine Calkins: We talk a lot in business about social licence. I think we need to start talking about social media licences to do things with peoples' information.

Dr. Ann Cavoukian: Yes, that's a very good point.

[*Translation*]

The Chair: Thank you. Your speaking time is up.

I will now hand the floor over to Mr. Andrews, who has seven minutes.

[*English*]

Mr. Scott Andrews (Avalon, Lib.): Thank you very much and welcome, commissioners.

I have four or five questions, and I'll pose my first three to Ms. Denham. You just briefly talked to—

[*Translation*]

The Chair: I will now give the floor to Mr. Tweed, who has a point of order.

[*English*]

Mr. Merv Tweed (Brandon—Souris, CPC): Thank you.

Mr. Chair, I apologize to our guests and to our committee, but I have a concern with the member who is now speaking. I think he owes this committee an apology, and we have seen that the media have apologized for their inappropriateness and breach of our committee that occurred last Tuesday.

I'm giving the opportunity to the member to apologize to the committee now, and we can move forward or we can deal with it as it moves forward. So I would open the floor for the member first to apologize to the committee for his behaviour at the last meeting.

[*Translation*]

The Chair: Thank you.

I heard your point of order.

I will therefore hand the floor over to Mr. Angus.

[*English*]

Mr. Charlie Angus: I'm sorry that this grandstanding is happening. There was a discussion in camera and you can call me out of order for it if you want. At that discussion, there was a gentleman's agreement that we would talk to each other and come back to the committee with a recommendation. Unfortunately, Mr. Del Mastro went into the House and made a public statement. Now you're using this on a televised broadcast to make a public statement.

This was something we agreed to deal with within our committee and then come forward with recommendations. So I think you're just trying to embarrass him.

I'd tell Mr. Andrews he should wait until we go back to continuing the conversation that we had on Tuesday.

● (1220)

[*Translation*]

The Chair: I will let Mr. Andrews decide what he wants to do. If he wishes to continue the discussion with the witnesses and to come back to this topic a little later, in accordance with the agenda, we can leave the matter there.

Mr. Andrews, you may continue.

[*English*]

Mr. Scott Andrews: Before you go into my time, maybe we should discuss this in public after our witnesses, and I'd be willing to address Mr. Tweed's comments at that particular time. I would not want to do it in camera as is suggested on our order paper. I will address that at a later point.

So can I continue with my questioning?

[*Translation*]

The Chair: Yes. You have seven minutes.

[*English*]

Mr. Scott Andrews: Thank you.

Ms. Denham, I have three questions for you. Mr. Calkins just talked about knowledge and consent, and one of the other things you mentioned in your presentation was limiting the use of the data that is collected. Do you have any suggestions on how one would regulate that? How do we limit one's use of the data that these companies collect?

The second question is this. You've talked about investigations, and you mentioned one. How many investigations have you undertaken, and have they been of the social media companies? I believe the one you referenced wasn't of the social media company but of an outside party that used the information.You can correct me if I was wrong in stating that.

In part of that you said you issued some guidelines to this outside group. I wonder if you could provide those guidelines to the committee. How extensive were those guidelines? Could you just clarify those few points.?

Ms. Elizabeth Denham: Absolutely.

In terms of ideas for limiting use by social media companies, obviously, people are voluntarily putting information online on their profiles. The company should only use that data for the purposes that are clearly stated, and that's the whole principle of transparency.

If the company then wants to use the information for a new purpose, then it has to go back to the users and explain the new purpose and get their consent. A really good example is that if you're a Facebook user and then all of a sudden Facebook rolls out its facial recognition technology software. That's a new use of the data. It's a more precise use of the data. It can lead to all kinds of function creep. I think in that case the company needs to go back and explain the new uses, the shiny new toys that are available to users, and get their consent.

That's really important. If they have new partners, if there are more third-party applications that are using the data, again, let users know and make it easy for them to say no or to control the use of their data.

The second question you asked me is about the number of investigations we have done of social media sites versus investigations that involve social media. I gave you the example of our investigating, really, the employment situation and how employers or third parties are making use of social media. I wanted to draw that investigation to the attention of this committee because I think it's really important to look at how social media is used by litigants, by law enforcement, by employers, by post-secondary institutions, because I think that's part of your study as well.

We've done several of those investigations, and I will share our social media background check guidance with you. I'll send them to the clerk of the committee for your review.

Mr. Scott Andrews: Thank you very much.

Ms. Cavoukian, I have a question on privacy by design. Has there been any discussion with the social media companies, Facebook and Google, on this very concept? Have they issued any opinions on this particular concept of privacy by design?

● (1225)

Dr. Ann Cavoukian: I've met with people and spoken at both Facebook's headquarters and Google's, and there is considerable interest in privacy by design. With regard to Facebook, if I had to guess their position, I would say they view privacy by design as being incompatible with their business model. That view is essentially, use as much information for as many purposes as you can, and then if you go too far—as they did with the news feed—then you can pull it back in terms of people's privacy preferences.

I have the greatest respect for Mark Zuckerberg. I've spoken to him. He totally gets that privacy is all about control, and I would suggest that he certainly values his privacy and controls it. But in terms of the business model, I think they would not be interested in it.

Google, on the other hand, is interested. If you look at Google+, which is their online social media, they have tried to incorporate privacy by design features. They invited me to speak to their head engineers, who were designing it, about privacy by design and how you incorporate this in terms of data minimization and making privacy the default. That was the concept behind “circles” and trying to minimize data collections.

I'm not going to oversell this. I think businesses will come to this gradually, if the business model is predicated on reaching as many people as possible.

Having said that, there is a way you can have online social media and privacy, and that's the Google+ experience in circles. I know many people who are on it. I don't know what the numbers are right now. I think they've exceeded 50 to 60 million, but we'd have to confirm that. It has an ability to restrict the information you share to the narrow audience that you want to share or speak with.

If I may, sir, I want to add one comment relating to your first question. With regard to the notion of minimizing data and collections and how you restrict it to the primary purpose, one example we did in my jurisdiction involved the creation of an enhanced driver's licence that could be used across the border instead of a passport.

They, of course, have to collect information. We put directly into the regulation what information, what personal identifiers, could be collected: the name, one's address. We said they should identify the fields specifically, as opposed to leaving it open-ended. We were able to do that. One way of trying to restrict the collection of personal information is by identifying specifically, very narrowly, that which you are permitting.

[*Translation*]

The Chair: Thank you.

Your time is unfortunately up, Mr. Andrews.

I am going to give Mr. Butt the last seven minutes. Time is passing, and the committee will proceed with its business afterwards.

[*English*]

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

Thank you very much, to both the Ontario and British Columbia commissioners for joining us today.

Maybe I'll start by asking each of you, are there specific things you are doing through your provincial legislation that we are not doing at the federal level that would improve our protection of privacy? Can you give me one or two specific things you are doing in your provinces that we could learn from and do a better job of?

As you know, there is a bill before the House right now that is looking at PIPEDA. I'm sure it eventually will get to a committee like this, where there will be some vetting to make it a stronger piece of legislation.

I'll ask each of you—we'll start with B.C and then go Ontario—if there's anything specific you can offer the committee that would be helpful around our federal laws and that would emulate what you are doing in your provinces?

Ms. Elizabeth Denham: In our discussion today we've been talking about how we need to get the law right. We also need to get the policy right. There needs to be incentives to get the private sector players on board. We also need public education to teach, especially, young Canadians how to properly protect their privacy online.

If social media companies won't play ball with Canadian law, then we really need strong enforcement because at the end of the day it's the essential tool to compel compliance. We can give all the guidelines we want, we can meet with companies, and we can give them great concepts of building privacy into their products, but at the end of the day we do have to have some teeth. We do have to investigate, and we do have to enforce.

In my view, order-making powers are the best starting point. I also think the mandatory breach notification increases the investment in protection of personal information and security and awareness.

● (1230)

Mr. Brad Butt: Dr. Cavoukian.

Dr. Ann Cavoukian: Thank you.

I concur with my colleague, Commissioner Denham.

We have order-making power in Ontario, and I'm telling you it would not be the same without it. But let me be clear—it is a last resort. The order-making power, which gives you the teeth, is the stick. We rely on it infrequently.

I'll give you the example of PHIPA, the Personal Health Information Protection Act, which applies to both public and private sector health organizations in Ontario, of which there are many. That was introduced in 2004. I've only issued 11 orders under that—so in something like eight years, 11 orders—because there is enormous incentive on the part of organizations to work collaboratively with us early on, and we always try to do that. We work very collaboratively. We strive to reach informal resolutions to investigations and problems, and we've had hundreds, thousands of them. It works very well. The carrot is a much better inducement when they know the stick is there.

On occasion we've had to issue an order and we do it not gladly but certainly willingly, if necessary. Often the order serves the purpose of an educative tool. It sends out a very clear message to everyone of what the standard of practice is now, and what our expectations are in this area. So order-making power is absolutely essential.

We have mandatory breach notification under PHIPA. That is also very important because that informs the population involved in the breach. It gives them the openness and transparency of knowing what is taking place.

We've also had, through the Regulatory Modernization Act in this province, a policy-led hook, if you will, in terms of looking closely at how you embed privacy-types of solutions into regulatory activities. So it's very important to have that cooperation.

I should also tell you, though, that my staff and all of us are out there regularly meeting with organizations. So not only is public education very important, but you have to meet with the organizations that fall under your jurisdiction so that they gain a better understanding of what your expectations are and how they embed privacy by design into their practices, into their technologies, and into their day-to-day activities.

They need to learn that from us, and we do this regularly. I think that allows us to minimize the number of orders we issue, but everyone knows the order-making power is there. It's a very powerful tool.

Mr. Brad Butt: As my last question, I'll ask you to comment on this. Commissioner Stoddart gave evidence in regard to the work product information that the national commission looks at, each matter on a case-by-case basis, as opposed to a specific definition. Can you talk about the specific definition versus what the federal government is doing, looking at matters on a case-by-case basis?

I'm not sure who wants to start, but it's up to you if both want to answer that.

Ms. Elizabeth Denham: For clarity, are you talking about the definition of work product information within PIPEDA?

Mr. Brad Butt: Yes, I believe so.

Ms. Elizabeth Denham: I think it's important to have a work product definition, because it takes out of the definition of personal information what might be actually just the product of somebody's workplace—an opinion that they write as a lawyer, a report they write as an engineer. To me, that's not personal information, that's work product information and should not be regulated under the act.

I think that's the question you're asking.

Mr. Brad Butt: Thank you.

Dr. Cavoukian.

● (1235)

Dr. Ann Cavoukian: I agree with Commissioner Denham that sometimes you're producing work at the workplace that has your personal information on it. It has your name and position, as it should, but it is not personal information as it is defined under our statutes, because it doesn't relate to you personally. It relates to your work and what you are required to do at your workplace. So properly, it should not only be identified but should be made publicly available.

I use myself as an example. Obviously I issue orders, and my name is on the order. I also issue many decisions, and my name is attached to them. It would be silly to say that it is my personal information. Obviously it has my personal identifier on it, but it's linked to the work I do and rightly belongs in the public sphere. Just because it has my personal identifier on it doesn't mean that it shouldn't be publicly available, if that's what you mean. It depends on how it's defined in the context.

[*Translation*]

The Chair: Thank you. Your speaking time is up.

I want to thank the two commissioners who agreed to appear and who gave us very informative presentations.

Ms. Borg, you had a point of order?

Ms. Charmaine Borg (Terrebonne—Blainville, NDP): In fact, as we are communicating with two very interesting witnesses, perhaps we could postpone committee business until the next meeting, next Tuesday, so that we can spend a little more time with these ladies.

The Chair: Is there unanimous consent on this matter?

There does not appear to be a consensus.

[*English*]

Mr. Chris Warkentin (Peace River, CPC): Was there a desire for a little bit of time? I know that Mr. Andrews wanted to make a statement at the end of the committee meeting. I don't know if that's something he wants to have reserved or if he would like to maybe do that in the House.

[*Translation*]

The Chair: That is his choice. We could continue for a few minutes and set aside five minutes at the end to discuss this matter again.

So we will reserve five minutes at the end of the meeting. According to the agenda, a five-minute question and answer period will be reserved for the commissioners.

In short, since you are very interesting, we are going to keep you with us a little longer.

Ms. Borg, you have five minutes.

Ms. Charmaine Borg: Thank you very much.

I am very pleased to be able to ask you some questions. You have a lot of information very relevant to our study. We will also be able to elaborate on issues such as how to protect our personal information in the database and in accordance with default parameters conducive to the protection of privacy.

Ms. Cavoukian, I would like to ask you a question on new technologies.

You said you were in the process of consulting a number of engineers, to whom you are explaining how to use the privacy models and to integrate them into the new technologies. Other witnesses have said that certain technologies accidentally collected information and did not make it possible to destroy data.

This is a bit new, but I would like to know how, at the national level, new technologies that are developed could include this integrated privacy protection model.

[*English*]

Dr. Ann Cavoukian: There are several things we can do. Obviously, raising awareness and education is our job, and we're getting the word out there strongly. You should know that internationally, word about privacy by design is growing. As I mentioned, in 2010 it was made an international standard. If you go to our website, www.privacybydesign.ca, there's a lot of information that we share regularly.

Most organizations do PIAs, privacy impact assessments, when a new technology or a new best practice or process is introduced. You can require, or certainly request, that in the PIA process, privacy by design is reflected. If I can again encourage you to go to our website, last year we had a PBD PIA. PBD is privacy by design. This PIA was specifically developed to reflect the requirements of privacy by design in the PIA. It's one of the essential tools in any practice. When you have a new technology or business practice, you do a PIA to identify the privacy risks and address them before the program or business practice becomes operational.

By requiring the seven foundational principles of privacy by design to be reflected in the PIA, and thereby reflected in the new program or business practice, you can be assured, at least, that the issues are being addressed. The kind of data minimization you were speaking to earlier that would speak to preventing unintentional access to the data used for other purposes, the harms that arise when data are used in ways that were never intended—all the problems we are so concerned about—can be addressed right from the beginning. That's the beauty of privacy by design. It tries to identify the privacy harms right at the initial stages, when the technology is emerging or the program is just being developed.

If you embed privacy protective features at the nascent stage, right at the beginning, it's much easier to minimize the harm and address it before the program is operational or the technology is fully operational. It makes a big difference. I would point you to the PIA process as an ideal place. Also, we have it on a CD. I can send it to anyone who's interested.

How do you do privacy by design? I was asked in 2010, when privacy by design was made an international standard, if my office could offer some assistance to other regulators around the world on how to do this privacy by design thing. How do you actually operationalize it?

We developed a curriculum that I think is very accessible. It walks you through the various steps of the principles and how you would do it. I make that available to anyone who's interested. We've shared it with many universities and Intel and other companies. All the tech companies have it. It basically walks you through how you do privacy by design.

Thank you.

● (1240)

[*Translation*]

Ms. Charmaine Borg: Thank you very much.

We would like to get a copy of that CD. That would be in the committee's interest.

You did not get a chance to explain how biometric encryption operates. Could you explain to us in detail how it works? How can we ensure that we are not collecting data on everyone who enters a building or browses a website?

[*English*]

Dr. Ann Cavoukian: Okay, I'd love to do that. It's really quite simple, though it sounds very complex.

Imagine your pictures being taken or your fingerprints being taken. The normal process involved in facial recognition programs or biometric programs is, as I said, to capture what is called a biometric template, which is a digital representation of the essential features of your face or your finger. That template is what is captured in the database and that is what is used for purposes of comparison.

The problem is, as I said, if the police come knocking on the door with a court order. You have to give them access to the database. They will be able to match that template of your face, the digital representation of your face, with a face that they might have taken a picture of at a crime scene. They get a match, and boom, your information is used for another purpose that was never intended.

Au contraire, with biometric encryption, what does it do that's different? It uses the unique features of your face or your finger to encrypt or code some other data: a PIN number, an alphanumeric, something meaningless, a nonsense number—it doesn't matter. And that biometrically encrypted data, this other data, is what's kept in the database.

So there are two things. If the police come knocking on the door, what do they get? You have to open the database to them. First of all they get nothing, because without your actual face present, one can't decrypt or decode what is in the database. So first of all, they can't get access to it even though you're going to open the doors.

Okay. What if there's a brute force attack? This happens. There are great hackers out there. What if they break into the database? What do they get? They get nothing of value. They don't get your face or your finger. They get this other meaningless nonsense number that was encrypted using the unique features of your face or finger, so they get garbage. Be my guest; they're not going to get anything of value. The beauty of it is that, for the purpose for which it was intended, it works perfectly. And if you go to our website, you'll see that the University of Toronto worked with the OLG, the Ontario Lottery and Gaming Corporation, to perfect the system. They reached levels of not only privacy but security and accuracy that were unprecedented for biometrics.

The large company Morpho out of Paris, France, which is the leading biometric company in the world—they just bought Sagem, which used to be the leading company; it's now Morpho—is looking at biometric encryption to develop a prototype, a pilot that it's going to be working on in the fall on how we can incorporate biometric encryption into a hardware device or something. So people are looking at this around the world. It's in its infancy.

But the beauty of the OLG example is that I can guarantee to all the regular patrons of the casinos in Ontario that they don't have to worry about their facial images being captured when they go out for an evening's recreation. I can also assure the addicted gamblers who want to be kept out that there will be a much greater success of having their wishes abided by through this program.

The success rate, if you will—it's called the hit rate—of the program of self-excluded people has grown, tripled and quadrupled. Before, we had very little for identifying these poor individuals. Now the success rate is through the roof, and there are something like 15,000 addicted gamblers in the province who have signed up for this program. We can help them do what they want us to do and keep them out, while not impacting the privacy of anyone else. And we've also told these individuals that, while they will be kept out of this program, their information will not be used for any other purpose whatsoever—no secondary use, full stop.

● (1245)

[*Translation*]

The Chair: Thank you. I'm going to have to stop you in order to give Mr. Calkins the last five minutes of speaking time.

[*English*]

Mr. Blaine Calkins: Thank you very much, Chair. It's Blaine Calkins day at the committee today.

Ms. Cavoukian, I want to explore this digital template you talked about. It sounds to me as if it's actually part of the encryption key. Do I understand that correctly?

Dr. Ann Cavoukian: Under biometric encryption, the encryption key would in fact be the facial image or the finger. The unique features of your biometric would become, in effect, the equivalent to an encryption key that would then encrypt some other data.

Mr. Blaine Calkins: But that encryption key, in order to be decrypted by a friendly user, would have to be known, so the multiplier for that encryption key would be what? The algorithm would be—

Dr. Ann Cavoukian: The decryption key resides on your face or finger. The biometric would be the decryption key.

That's why, if the police came knocking at the OLG, they could say, “You're welcome to the database.” They don't possess the decryption keys. The decryption keys reside on the facial images of the individuals participating in this program.

Mr. Blaine Calkins: That's good. It brings a new meaning to the words “destroy the key”. I guess we're going to have to be a little careful there. It was very comforting to know that my facial image was of little or no value, but I know you didn't mean it that particular way. I'm just being silly, of course.

Thank you for that explanation. I understand it perfectly well. It's how I suspected it was going to work.

I want to talk about the deletion of information. I was an Oracle database administrator. Whether it's a relational database or whether it's an object-oriented database, whatever the case may be, the data is stored in various forms, depending on the system being used. Very often, in the design of user interfaces and so on, information is collected, or sometimes we ask for our information to be taken out of a database, and the difference between deactivation and deletion is quite significant because we can deactivate records. We can make it look as if somebody is no longer a customer, no longer a client, but we still retain all the data for past transactions in the database.

We may be required to keep that information for tax purposes, for various legal or statutory reasons. But at some point in some of these transactions, where people's privacy is given up for the use of free application software on a mobile application, that's a completely different transaction.

I'm wondering if you, Dr. Cavoukian, or you, Ms. Denham, can speak about what you do when a user or a citizen requests the deletion of information. What can be done to better protect those Canadians?

● (1250)

Ms. Elizabeth Denham: That's a very important question. A basic privacy principle is the right to be forgotten, so in our laws, organizations can only retain information as long as they need it for business purposes and then it should be destroyed.

I led the Facebook investigation in 2009 in the federal office, and this was a real sticking point in that investigation. We found quite a difference between deactivation of someone's account and deletion of the data. The recommendation coming out of the federal commissioner's office was to make it easy for people to delete their accounts, and be clear on the difference between deactivation, which is really putting the data offline, just in case the user changes her mind down the road and wants to be back on Facebook, versus deletion, which I believe takes about 30 days and then all the data is deleted.

We wanted the company to make it really easy for individuals to choose which option and to make sure it's done.

Getting back to order-making powers, the federal privacy commissioner is an ombudsman, and she can make recommendations. At the end of the day, my colleague Ann Cavoukian and I, with our order-making powers, can order a company to delete data, and it has to do so within 30 days. Under my law it's 30 days. That is a very powerful tool.

Dr. Ann Cavoukian: Thank you, Commissioner Denham. Like you, we have order-making power, and we can order the cessation or the destruction of collections of personal information that have been collected contrary to the act.

I did that a few years ago with the Ottawa police, believe it or not. They had collected information that I ordered destroyed. I had the pleasure of meeting Vern White, who was then the police chief in Ottawa and is now Senator White.

So we do have, in terms of what comes under our jurisdiction, the ability to order the destruction of these collections. Then we can ask for third-party audits to ensure that the data has been destroyed, although I had no concerns with the Ottawa police doing so.

As Commissioner Denham mentioned, the right to be forgotten is extremely important. It features prominently in the new EU data protection regulation that has been drafted.

Also, it is becoming more and more important because of the limited control you have in online social media and other fora in terms of online access. Is it really being destroyed? Is it being deactivated? How long...? What assurances do you have?

I'm going to suggest to people that you have very few or virtually no assurances in terms of private sector information that exceeds, certainly, my jurisdiction, and that may exceed others' jurisdictions. Even our ability to audit is very difficult to do. It takes a lot of effort. What the FTC and other organizations are doing now is building in the need for independent third-party audit, so that if the destruction of records has been ordered or required, it can then be confirmed after the fact.

But I just want to point you to one thing, and I'll say this as my final comment. Over time, I think it's going to become increasingly more difficult if companies and governments don't follow privacy by design in terms of proactively offering privacy as the default feature. You're not going to be assured of privacy or a destruction of your records. It's going to be a free-for-all.

We've been working with the University of Toronto to develop a new concept called SmartData. If you go to our website, you'll see that we just had an international symposium on SmartData, which is the developing of virtual tools that will work for the data subject and will be your virtual agent online to protect your data and act on your behalf in a contextual way.

I'm not going to take any more of the committee's time, but I just wanted to point you to SmartData. You can go to it on our website or we can send you some information. Again, we're calling it the embodiment of privacy by design—to basically give consumers, the users, the tools that will enable them to also protect their own data.

Thank you.

● (1255)

[*Translation*]

The Chair: Thank you. Thank you a second time for being available to make your presentations today.

I hope we will be able to access the document you mentioned, Ms. Cavoukian, and that we can forward it to every committee member through the clerk. Thank you for being here.

We will suspend proceedings for a few minutes and then, as you know, come back for the last five minutes to talk about committee business.

Thank you.

● (1255)

(Pause)

● (1255)

The Chair: We will resume the meeting.

Mr. Andrews wanted to say a few words.

[*English*]

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

As committee members know, I did apologize in camera at our last meeting, and I will do it in the public portion of the meeting. That's why I asked that we stay in public.

My apologies.

[*Translation*]

The Chair: Mr. Andrews apologized here in public.

Is there something else on the committee's business agenda that we wanted to discuss?

I wanted to make a few announcements. In particular, I submitted the report of the Société du Vieux-Port de Montréal this morning. So it has been tabled in the House.

The correction that we wanted to make to the lobbying report has also been made. It has been accepted by the House by unanimous consent. That is what I wanted to tell you.

Did Ms. Borg want to add something?

[*English*]

Mr. Charlie Angus: I just wanted to follow up on the other day—

Ms. Charmaine Borg: Okay.

Mr. Charlie Angus: Sorry.

Because there were two incidents the other day, and I'm concerned about the protocol with media. Because what happened to Mr. Andrews could happen to anybody when you're not paying attention. You're focused, and if someone taps you on the shoulder and says, hey, what do you have...? I'm just concerned.

It might have been...you know, the media might not have been paying attention, but do we have a protocol in terms of the role, of the limits, of journalists who approach the table while we are doing our work?

Because I think we need to just make that a clear position—that while we are doing the work of the ethics committee, we should not have journalists coming up and tapping us on the shoulder while we're working. I think we need some kind of.... We don't need to make a big statement, but we have to have a clear working understanding about how we're going to work together.

[*Translation*]

The Chair: The clerk tells me that certain existing rules are supposed to govern the work of journalists in committee meetings. I am going to hand the floor over to him.

[*English*]

The Clerk of the Committee (Mr. Chad Mariage): Thank you, Mr. Chair.

In February 2009, a memorandum of understanding between the parliamentary press gallery and the House of Commons was reached. It was based on an initial report and a trial run that was a result of a study done by the procedure and House affairs committee.

I can distribute that directive to members, if you're interested.

[*Translation*]

The Chair: Mr. Harris, you have the floor.

[*English*]

Mr. Richard Harris (Cariboo—Prince George, CPC): Just as a point of clarification, I believe within the protocol it is not permissible for a reporter, a member of the press, to come and interrupt a member sitting in a committee meeting. Is that correct?

If that is the correct protocol, and it certainly must be understood by the reporters who work on the Hill day after day, then there was a breach of protocol by that reporter who did approach a member. Whether she caught him by surprise or not, she bears a lot of the responsibility.

This committee, if she's breached protocol, would be well in its right to issue a complaint via the Speaker, or directly against her, and remind her of the protocol and not to let it happen again.

[*Translation*]

The Chair: Mr. Butt, do you wish to add something?

[*English*]

Mr. Brad Butt: That was basically my point. I think there is a rule right now about reporters approaching the committee table while committee's in session. It's absolutely prohibited. That's my understanding, and that's what it should be.

The reporter should have known the difference. I think she did catch Mr. Andrews off guard, and I think that was unfortunate. I think I would agree with Mr. Harris that the reporter bears very much the blame. She's not brand new around here. She's been around here quite awhile, so she clearly knows what the rules are.

I don't think there's any question that this is the rule. You do not approach the committee table while committee is in session—period.

● (1300)

[*Translation*]

The Chair: I would like to add that we normally do not allow journalists to be around the table during a public meeting. Perhaps we could remind journalists of those rules through the president of the Parliamentary Press Gallery in the House of Commons. We could remind them of the rules, Mr. Andrews.

[*English*]

Mr. Scott Andrews: It would be helpful for the committee to have a copy of those rules. I think you just referenced a document.

You guys also referenced something.

I don't believe I've ever seen that document. I'd like to have a look at it.

[*Translation*]

The Chair: We can distribute it immediately or by email, if you wish.

Mr. Angus, you have the floor.

[*English*]

Mr. Charlie Angus: Just to finalize this, you're the one with the gavel here. You're the one who holds order. Whether we issue a statement....

I don't know if we need to go well beyond. I mean, it was a breach. I don't think it was something that.... It could have caused damage, but I don't know if we want to take it too far.

Whether you as chair put it in writing, or you issue a clear statement that from here on in it will be understood that, at our committee, this will not happen, we just need to have that on the record so that when anyone looks at it, we heard it, we dealt with it, and it was addressed by you, as our committee chair.

[*Translation*]

The Chair: With the committee's consent, obviously, I can write a statement to be sent to the Parliamentary Press Gallery informing it of the problem regarding what has happened. I could have that statement approved by the committee before sending it.

Mr. Calkins, you have the floor.

[*English*]

Mr. Blaine Calkins: I'm not certain we need to do that.

I think what we've heard clearly is an apology from the member of the media in question. That is an admission that she understood the responsibility that she had, and that she breached that responsibility that she had. She's apologized for it. I'm satisfied with that.

Mr. Andrews has now apologized publicly for that same issue.

It's an unfortunate issue, but as far as I'm concerned, I think everybody who's paying attention to this now understands clearly what needs to happen from a go-forward perspective.

I would be just as satisfied that we put this behind us.

[*Translation*]

The Chair: I believe there is an agreement to leave the matter there. As Mr. Calkins mentioned, journalists may perhaps pay a little more attention in the future. This will have taught everyone a lesson.

Ms. Block, you have the floor.

[*English*]

Mrs. Kelly Block (Saskatoon—Rosetown—Biggar, CPC): I know it's time for the committee to end, but as a non-sitting member who's joined you today, I'm wondering if it wouldn't be beneficial to have that same document circulated to the other committees. They may not be aware of the very same rules that you have had to deal with here.

Perhaps it could be recommended to the other committees that if they'd like to receive that document, it could be made available.

[*Translation*]

The Chair: That can definitely be done by the clerk, who has that document. He can contact the senior management of all the committee clerks to ensure that the rules are clear and are forwarded as efficiently as possible to all members and journalists, who must also be aware of them.

Is there anything else on the agenda?

It is already 1:04 p.m. The meeting is adjourned.

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