



HOUSE OF COMMONS  
CHAMBRE DES COMMUNES  
CANADA

# **Standing Committee on Access to Information, Privacy and Ethics**

---

ETHI • NUMBER 043 • 1st SESSION • 41st PARLIAMENT

---

**EVIDENCE**

**Tuesday, June 5, 2012**

—  
**Chair**

**Mr. Pierre-Luc Dusseault**



## Standing Committee on Access to Information, Privacy and Ethics

Tuesday, June 5, 2012

• (1100)

[Translation]

**The Chair (Mr. Pierre-Luc Dusseault (Sherbrooke, NDP)):**  
Good morning, everyone.

The witnesses on our agenda are Mr. Everson, from the Canadian Chamber of Commerce, and Ms. Pettit and Mr. Wycks, from the Marketing Research and Intelligence Association. Thank you all for being here today.

Let us start right away. You will each have 10 minutes to make a presentation. Then we will move to question and answer periods, when the committee members can ask you questions.

Mr. Everson, you have 10 minutes.

[English]

**Mr. Warren Everson (Senior Vice-President, Policy, Canadian Chamber of Commerce):** Thank you very much, Mr. Chairman, and thank you to the members of the committee for calling us and providing us with an opportunity to speak on a fascinating issue before you today.

This is a very important topic for Canada. I very much think it behooves the committee to examine its complexities, and it's to your credit that you're doing so.

The Canadian Chamber of Commerce has long followed the debates about privacy in cyberspace. Last year, delegates at our annual policy convention passed a resolution called "Private Sector Privacy", which speaks directly to the issues you will be discussing here. When I'm finished my statement, Mr. Chairman, I'll provide that to the clerk in both official languages, if you'd wish to have it in the record.

The key sentence of the resolution, however, for this committee might be the one that states:

PIPEDA allows for an effective and workable balance between...protecting an individual's personal information and allowing business to operate....

Surely, that's the issue most central to your deliberations.

This is a very significant attribute for legislation in such a fast-moving sector of the economy and one that we should be careful about disrupting.

I would encourage you, as you begin your work, to heed the advice given to doctors, "First, do no harm".

Social media and privacy, obviously, are very much in the news these days. This is understandable, because millions and millions of

Canadians and hundreds of millions of people around the world are using new technologies and social platforms, and sharing information about themselves. That, of course, raises important questions about privacy and policy.

I want to make two brief remarks in my comments. The first is that the rules for privacy in Canada are well-known, they are well understood, and in my estimation they work. They have adapted remarkably well in the digital world, and they provide quite strong protections for Canadians. It's a tribute to the people who drafted a law years before anybody knew about Facebook, Foursquare, or Twitter that their work is still relevant and helpful to us today.

Secondly, social media is experiencing a very dramatic growth. It's attracting millions of dollars of investment in Canada's digital economy and is creating thousands of jobs in Canada. These can be very high-quality and well-paying jobs. So while it's entirely appropriate for the committee to be attentive to concerns about privacy, the committee's review, in my view, should be in the context of highly successful innovations that are serving an ever-growing population. My summary there would be that social media is a good news story in Canada.

Canadian privacy law works. It does protect consumers.

More than a dozen years ago, when PIPEDA was passed, the law was intended to be technology neutral. I think it should be understood as a statute that was designed to encourage business online, experimentation and innovation, while providing consumers with considerable choice about how their information would be collected, used, and disclosed.

PIPEDA is based on the important concept of reasonableness, which sets a baseline for businesses and the expectations of Canadian citizens. Collection, use, and the disclosure of personal information has to be reasonable in the particular circumstances. Not every law is like this, but this one has stood the test of time.

Circumstances obviously evolve. The framework in which PIPEDA is applied similarly evolved to take into account how citizens and businesses are participating in the online world.

The Chamber of Commerce, then, is of the opinion that there is nothing in social media that stretches PIPEDA to the breaking point.

We've had almost a dozen years of experience with the current rules, and we have found that innovation can take place under the umbrella of its flexible and principled regulation.

The true potential of the Internet is a level playing field on which Canadian businesses can compete globally but is one that can be retarded by excessive regulation and ultimately would come at the cost of Canadian jobs.

I would like to tell you, just quickly, about a couple of companies, a few companies, that are operating in this space and about the jobs that we've seen created. I'm doing this partly because our preoccupation with the Internet is always with monster companies that are household names, and many of those are members of the Canadian Chamber of Commerce and I'm glad to have them. But there is a story that is not often told to tens of thousands of Canadians in ridings all across the country whose livelihood depends on social media.

HootSuite was founded by an entrepreneur in Vernon, B.C. It makes a social media dashboard that aggregates information from a lot of different sources. HootSuite was an official partner for Google and Pages launched last year. HootSuite has attracted a blue chip list of clients, including the White House, Dell computers, and Disney. I wouldn't be at all surprised if many of your campaign managers were using it to connect with constituents during elections.

HootSuite has received more than \$20 million in direct investment and is seeking another, I think, \$50 million. It is a home-grown company that's now worth close to half a billion dollars and it employs 140 people.

Radian6, a start-up in Fredericton, was one of the powerhouses in social media. Now it has offices in New Zealand, the United States, and the U.K. Their products enable companies to understand what's being said about them on the Internet and across a range of social media. They've received millions of dollars in investment and they've hired hundreds of Canadians. Radian6 was bought by an American company last year for \$326 million, but it's just as strong as it's ever been in Canada, and it's continuing to hire more people.

• (1105)

Until I prepared for this testimony, I had never heard of a company called Bight Interactive in Charlottetown, but Bight saw the potential for online social gaming and authored a game called *Trade Nations*, which is played by thousands of people around the world via Facebook. Bight Interactive was recently acquired by one of the largest video companies in the world, thereby injecting significant capital into Prince Edward Island.

A final example here is Frima Studio, which was founded in Quebec City in 2003 by three entrepreneurs who wanted to make video games. It was a very humble beginning in a single studio apartment where they were living. But Frima has created games more recently for Hollywood brands like Harry Potter and Looney

Tunes, and their growth has been so significant they've opened a second studio. What I like about the cyber world we live in is that the second studio is in Matane, on the Gaspé Peninsula. We're very geographically indifferent in the modern world. With 265 full-time employees, Frima has been at the forefront of this trend toward social gaming. They've created a lot of quality, high-paying jobs in Canada, and among their many dozens of titles are multi-player social games and a lot of educational and training games. Training is a big preoccupation with them now.

We see social media experiencing a lot of dramatic growth, attracting millions of dollars of investment in Canada's digital economy, and creating thousands of jobs. Instrumental in this is encouraging the entrepreneurial work of Canadian innovators who are able to build these businesses to the global stage.

I started my statement by complimenting the committee for taking on this challenging topic. I certainly realize you have a responsibility to address concerns about the privacy of Canadians, but I would ask that you approach your work with a positive view of a fascinating sector, which is creating value for consumers and jobs for Canadians at an astonishing rate.

Thank you very much, Mr. Chairman.

[*Translation*]

**The Chair:** Thank you for being here and for your presentation.

I give the floor to the representatives from the Marketing Research and Intelligence Association, for 10 minutes.

[*English*]

**Mr. Brendan Wycks (Executive Director, Marketing Research and Intelligence Association):** Good morning. I'm Brendan Wycks and I'm the executive director of the Marketing Research and Intelligence Association, or MRIA for short.

With me is MRIA member Annie Pettit, who is vice-president of research standards and chief research officer at Conversion, a leading provider of social media research in Canada. Annie holds a PhD in experimental psychology and is regarded as an authority on research data quality, its relevance and reliability. Annie was also one of the Canadian representatives who was at the table in a global research industry associations initiative to develop social media research guidelines, which we'll address a little later in our presentation.

I'd like to start off by thanking the members of this committee for inviting MRIA to appear before you today and giving us the opportunity to present our industry's views on the matters you are considering.

First, a quick bit of background about MRIA. We are the national, voluntary self-regulatory organization that governs and represents both individual practitioners and companies in all sectors of Canada's marketing, survey, public opinion research, and market intelligence industry.

Our membership comprises more than 1,800 individual research practitioners and close to 400 corporate members. Our corporate membership is made up of small to large research agencies, which are suppliers of research services, along with many buyers of research services, such as financial institutions, major retailers, insurance companies, telecommunications firms, packaged goods companies, pharmaceutical firms, and other manufacturers.

As you will hear from Annie, social media research is a rapidly growing area of our industry. More and more, public policy and corporate decision-makers look to our members to help them gain a better understanding of Canadians through their digital activity, and in particular a better understanding of the opinions they share online.

MRIA is very supportive of this committee's initiative to undertake this important and relevant study. In that connection, it's an absolute priority for our association that our members adhere to high and rigorous standards, particularly when it comes to protecting the personal information of Canadians, whether on a survey telephone call, at a focus group, or online. And we would hope Parliament will help ensure that all other industries treat privacy protection just as seriously.

As you consider the testimony from various witnesses, we ask you to keep in mind the following with respect to our industry. There are three main characteristics that define marketing and survey research and that differentiate our work from other industries, such as social media marketers.

First, legitimate survey researchers never attempt to sell anything or solicit in any form. In fact, solicitation violates our rigorous code of conduct and good practice.

Second, we have a long history of industry self-regulation that has been recognized as effective by lawmakers in Canada and that has formed the foundation of a positive and productive trust relationship we enjoy with Canadians, trust that has been earned over many decades. In that connection, MRIA was the first marketing research industry association in the world to develop a charter of respondent rights, which we launched here on Parliament Hill in October 2006.

Third, survey research gives Canadians an opportunity to voice their opinions and to influence public policy and corporate decisions that will affect their lives, thereby serving a valuable societal purpose.

With regard to social media research specifically, MRIA has been an instrumental player in a global initiative to develop guidelines around ethical social media research. This initiative has been led by our counterpart organization in Europe, ESOMAR, with participation and input from MRIA and several other industry associations around the world.

Annie Pettit was one of two Canadian representatives from MRIA to participate in that important work. MRIA is now in the process of

codifying those social media research guidelines and building them into our standards code, with which our members must comply.

I'm going to hand off now to Annie, who will provide an overview of the types of activities our industry undertakes in the digital world and of the many safeguards our members observe to protect the privacy of online Canadians. After Annie's remarks, I'll provide a brief conclusion.

● (1110)

**Ms. Annie Pettit (Vice-President, Marketing Research and Intelligence Association):** Thank you, everyone, for taking the time to meet with us.

As Brendan said, my name is Annie Pettit, and I'm the vice-president of research standards as well as the chief research officer at Conversation, a Canadian start-up specializing in social media research. Because I'm seen as a global thought leader in the social media research space, ESOMAR in Europe, the Council of American Survey Research Organizations, or CASRO, and the Marketing Research Association, or MRA, the MRIA's counterpart in the U.S., each invited me to be a contributing member of their social media research committees.

To give you a sense of the role that social media research is playing in the market research industry, I would like to share with you just a few results from the spring 2012 "GreenBook Research Industry Trends Report", a survey of more than 800 market researchers around the world. Of those researchers, 28% have used social media research, 59% plan to use social media research next year, and more than 10% say that social media research is one of the greatest opportunities for researchers in the future.

Social media research is defined as the application of traditional market research principles to the collection and analysis of social media data for the purpose of better understanding policies and opinions. Just as survey researchers use survey data, social media researchers use social media data, and we apply the same strict methodological practices to that data.

For instance, as with traditional survey research or focus group research, just as survey researchers decide which people are best suited to participate in a survey, social media researchers decide which websites or online forums are best suited for understanding opinions. We incorporate traditional aspects of market research, including sampling, weighting, scaling, norms, and box scores to ensure that we measure opinions as accurately as possible.

The main purpose of social media research is to better understand the opinions people have regarding policy issues, products and services, celebrities and politicians, social issues, and cultural activities. Social media research helps us learn what people like and don't like so that we can improve the services and products people receive, create better products, and better serve our constituents.

Most importantly, social media research is not a kinder, gentler word for social media marketing. We do not market products; we do not sell products. We, like our counterparts working on the traditional side of the industry, conduct market research. We abide by and respect the same methodological and ethical guidelines and standards as traditional researchers.

I'd like to share with you just a few examples of how we abide by those principles. First of all, we take great care to only collect public data. Some websites, such as Facebook and LinkedIn, hide portions of data from outsiders, including Google. If you were to do a Google search, this data would not be found. Social media researchers do not and in fact cannot collect this data. In some cases we could just create a password and collect the data, but we don't; we respect that privacy.

Other websites allow anyone to read the entries. Comments left on YouTube, Flickr, or WordPress are written for strangers to read and enjoy and can be found via a Google search. This is the type of data that social media researchers collect. In addition, we depersonalize data that is shared in reports. We do not engage with social media users without their consent and we do not knowingly collect data from minors.

The Internet has evolved rapidly in recent years. Ten years ago it seemed incomprehensible for the average person to share intimate details of their life online. Today, bloggers are regular people who get excited when strangers, not their friends and family, read their thoughts and share them widely. Public forums are open social networks where strangers from around the world find and share opinions with each other. Twitter is a newer entrant into the social media space, and for many people using it, the ultimate goal is to read a tweet that millions of people around the world will read.

Social media has become so ingrained in our lives that users expect companies to respond to social media comments written in obscure corners of the Internet. People expect their social media complaints to be met with letters of apology from the companies they write about.

- (1115)

Right now, Canada is one of the global thought leaders in social media research space, and I'm proud to represent Canada in that role. But I worry that if we lose this position, if we are unable to compete in the social media research space because our privacy standards restrict us rather than let us self-regulate, our clients will have to use social media research conducted in places with less-than-high ethical standards. That scares me.

Let us be thought leaders. Let us continue to lead in the social media research space. Let's demonstrate to other countries that social media research can be conducted in a way that is beneficial to the

government and corporate decision-makers, to research companies, and most of all to Canadians.

**Mr. Brendan Wycks:** To sum up, MRIA prides itself on being a leader by adopting some of the strictest codes of conduct and standards globally when it comes to the protection of personal information. This is a key pillar in maintaining our industry's bread-and-butter, *sine qua non* relationship with Canadians, a relationship rooted in trust and goodwill and articulated in our "Charter of Respondent Rights", our industry's covenant with Canadians.

In the digital world, legitimate survey researchers take great pains to respect the rules of the social media sites we monitor, respect the wishes of those who post personal information online, anonymize the personal information in the data we collect, and never attempt to sell anything or solicit in any form.

The experience of social media research practitioners tells us that from the perspective of social media users, most Canadians who publish information online are quite informed about what they are doing. They have a good understanding of the impact of their actions and they know what steps to take to protect their personal information. It is our belief that high standards-based ethical business practices, combined with the informed, deliberate actions of Canadians when they post information online, constitute the right balance and the golden mean that ought to be maintained.

It's the right balance because it protects the privacy rights of Canadians in the digital world while also ensuring that social media researchers can facilitate their ability to have a voice and ensure that their views have influence in public policy and corporate decisions that will affect their lives.

Legislators have long recognized the survey research industry's ethical practices, and we firmly believe that we continue to maintain and adhere to the highest standards for privacy and the protection of personal information in the digital social media world.

For the committee's reference, we will be submitting as part of our written brief a copy of the industry's global guidelines for ethical social media research, which our association is in the process of codifying and which we suggest could serve as a best practices reference document for this committee's future review of PIPEDA.

Finally, let me close by saying that MRIA very much appreciates this opportunity to present the views of the marketing and survey research industry to the House of Commons standing committee on this important study, and we look forward to learning of its outcomes.

Thank you.

● (1120)

[Translation]

**The Chair:** Thank you very much for your presentation.

Let us now move immediately to the question and answer period.

Ms. Borg, you have seven minutes.

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

I would also like to thank our witnesses for being with us today. It is a pleasure to listen to what you have to say.

We have heard from witnesses who have told us that, especially among young people, there is a lack of confidence in social media companies. They are afraid that the companies are using their personal information. In general, they seem to think that, when you provide your personal information, they are going to be used. According to some witnesses, there is a loss of confidence in the area in general.

We have also seen, for example, Facebook shares falling dramatically. That shows a lack of confidence, in a way.

Where does the lack of confidence come from? How can we rectify it? Mr. Wycks and Ms. Pettit, you explained that you use best practices. But there are certainly other research companies that use bad practices. Does that affect you negatively? Can you comment on that?

[English]

**Ms. Annie Pettit:** I'm happy to speak to that question.

About a year or two ago there was a prime example of that by one of the well-known market research companies, whereby they entered a walled garden or a website that had permission-based access to it. They entered that website and scraped some data. It's the Patient-sLikeMe issue, if you've already heard of that. That was done by a well-known market research company. When that information was discovered, it was made public by *The Wall Street Journal*. That company received a lot of flak from its fellow market researchers in front of all their colleagues, at conferences, and online. It was well publicized.

This is the sort of the thing that is not tolerated. Anyone who is a part of the recognized associations has no patience for this kind of thing and does not tolerate it. This would be sanctioned under our current codes.

When that event did take place, there were guidelines in place by the MRA, the U.S. Market Research Association, that would have outright stated that that's just not appropriate behaviour.

Other industries do not share the same kind of motivation we have, but we know it is extremely important. It's near and dear to our hearts. We're looking to parliamentarians to make sure the Canadian privacy framework remains rigorous and robust as we continue to move forward in the digital world.

[Translation]

**Ms. Charmaine Borg:** Thank you.

Under PIPEDA, should the commissioner be able to impose financial penalties on companies that breach the code and the principles?

[English]

**Mr. Brendan Wycks:** Yes. MRIA's view is that we are supportive of stronger enforcement powers for the Privacy Commissioner of Canada.

[Translation]

**Ms. Charmaine Borg:** Thank you.

You mentioned that you always obtain the users' consent in order to conduct your research. We have heard that it is often difficult to obtain specific consent from one Internet user or one social network. How do you get that explicit consent?

● (1125)

[English]

**Ms. Annie Pettit:** In the case of social media research, or listening research, it is purely observational. We look and see what people are doing.

Where consent comes into play is where people want to have an interaction or engage with consumers, and that is totally a separate part of market research. In those cases, there would be some...if it's possible to determine who the person is, there would be some kind of communication: "May we engage with you? Would you like to speak with us?" Those are totally permission-based types of research.

In our case, we don't do that sort of interaction. Social media research is simply listening to what's going in the online space, observing but not formally engaging.

[Translation]

**Ms. Charmaine Borg:** For example, when I decide to set up a Facebook account, I check a box saying that I accept the conditions of their privacy policy. Is that what you do to obtain consent, ask a user to check a little box?

[English]

**Ms. Annie Pettit:** There are additional privacy settings in Facebook. You can determine if some or all of your Facebook data is allowed to go outside of Facebook. If you check the boxes that say your data can be public, can go outside of Facebook, then that is the kind of data we could access via social media research.

But a large percentage of data in Facebook is actually private. Social media research does not have access to it, just because people have checked that privacy box.

[Translation]

**Ms. Charmaine Borg:** I have another question about anonymity. How do you ensure that the information that you obtain and use remains anonymous?

[English]

**Ms. Annie Pettit:** That's an interesting question. A lot of people assume that when they write something in social media, their whole life is present for anyone to see.

Pieces are present. For example, you might sign up with a user name, you might provide an e-mail address, you might provide geo-location—Canada, Alberta, or something like that. In most cases it's a very tiny bit of information that is released. As social media researchers, we pick up that data, where it is available, for the purpose of aggregated data, so that we can say this percentage of people from Alberta share this opinion or this percentage of people from Ontario share this opinion.

If the information goes beyond that, in terms of a written report to a client, we take great efforts to make sure that whatever personal information shows up in it has been completely masked. There are no user names in reports, no photos, no e-mail addresses. Even in what someone has written as a tweet or a status update, the wording has been tweaked so that you can't identify what the phrase was originally. If someone were to have said "I really love Nike shoes", the phrase might be transferred into "I really like Nike shoes". It's just a few minor words, so that the general phrase is still there but there's really no way to match it back to the person who originally gave that information.

[Translation]

**The Chair:** Unfortunately, your time is up.

We now go to Mr. Del Mastro, for seven minutes.

[English]

**Mr. Dean Del Mastro (Peterborough, CPC):** Thank you very much, Mr. Chairman. Thank you very much to the witnesses.

First, Mr. Everson, I agree with your assessment. These are very important economic developments. I think the benefits are far- and wide-reaching. We see them in every region of the country and in every city and community in the country. I think it's important for business and I think it's important as far as a growth tool for business is concerned.

However, I'm interested in whether the Chamber of Commerce has looked at the issue of informed consent. I'm going to raise the same question with the marketing research association as well.

In my opinion, because so much legalese goes into social media sites and an awful lot of laymen use them, including me, who may not understand the impact of the boxes they're checking and what the intent of the statements is that they're signing off on, an awful lot of people scroll through disclaimers to get down to the box that says "Yes, I agree" and move on.

I'm just wondering whether the Chamber of Commerce looked at the issue of informed consent with respect to privacy.

• (1130)

**Mr. Warren Everson:** We didn't opine on it in a resolution, but of course we have a lot of debate about this in the relevant committee and within the chamber. I noticed that when the commissioner was here she was using the term "meaningful consent" to deal with a constituency of people who may not be competent to give their consent or understand the implications.

I would make a couple of points on what you said. On the legal gobbledygook issue, I think we all understand why it exists: somewhere a lawyer is trying to make his or her client bullet-proof against any possible action against them. It would be nice if the committee were to opine that it was time to clean up that language and make it simpler, putting that challenge before the attorneys.

As for the issue of meaningful consent, I don't know a more thorny issue in the world of cyber-commerce or one that I will be watching with more excitement to see what you come up with. The nice thing about being a member of Parliament is that if you're not an expert in any one field, you're an expert in the application of common sense, and this is where you're going to be with this issue.

If somebody is too young, is it the vendor or the carrier's responsibility to ascertain that? And in that case, how can they do so without unwarranted intrusion into their privacy? It's an extremely difficult challenge. I keep saying that someone bought them a computer, because if they're 13, they likely didn't buy the computer themselves, so there has to be some societal construct around them that might be employed.

It is an extremely demanding issue and one for which, as I say, the most obvious solutions, for the middlemen involved, are quite significant intrusions into our privacy, and we probably wouldn't be very happy about that.

Have I answered your question?

**Mr. Dean Del Mastro:** I think you did. I can say, having taken a number of university-level business law courses myself, that one of the first things you learn is that terms in law do not necessarily mean what they mean in everyday life. This is why, when you actually sit down and read one of the privacy statements or one of the statements you're signing off on, if you actually read them, you may have a lot more questions if you've taken a couple of law courses than you do if you haven't.



I can tell you, having read them, that I'm not entirely clear on what some of the subsections are getting at. I will ask that of companies when they come in, because I don't think it's your place to answer that. But I do think there is a role for clear language in working with the public, especially when we're talking about children or young people who might be using social media.

To the Marketing Research and Intelligence Association, I agree with you that research is very important, but again it comes back to an issue of informed consent. I respect that you're saying you don't sell anything and don't advertise anything. But you're giving all your research to people who do sell things and advertise things—that's who the customers are—and they're looking to use your research.

It's very important research, because one of the things that retailers are looking for today is how to reach a customer. And it's not just retailers, but others. How do you get a message to somebody in an era when we're not sure they're watching television, not sure they're listening to local radio, or reading local newspapers. They might be doing all of those things; they might be doing it online.... So the research you're doing is very important.

But it comes back to this question, and this is my concern. There's all kinds of medical research we could do that could be very important. We could in fact look at the medical records of every member of Parliament to determine whether running 16 hours a day and eating whatever is put in front of you is good for your liver. I suspect it's not. But you'd have to have their consent to look at those issues and to look at their medical records, to see whether it is okay.

If you just looked at the medical records and came back with helpful information, it might be good that you have the information, but the way you received that information in order to process it might be entirely wrong. This is the issue with respect to informed consent. If you're researching things from social media and are producing good data from it but are doing so in a fashion whereby a lot of folks....

If you had a focus group and you sat down with folks and said, "Did you understand that it meant this, this, and this?", I expect most people in the room would say "Yes, I knew that", because people aren't about to tell you that they had no idea what the legalese meant and they don't want to seem, for whatever reason, incapable of understanding it. They're probably going to answer affirmatively, if you just ask them if they understood that this is what they were signing on to. But I'm not confident that people always do understand the implications of what they're signing off on.

Would you support a move toward more common language and clarifications with respect to privacy and then abide by it? It sounds as though you're very keen on abiding by all of the privacy guidelines of social media. Do you see that there is an opportunity for people to be confused about people providing consent that they don't mean to be providing, and that there's a role for this committee in working to clarify it?

• (1135)

**Ms. Annie Pettit:** We absolutely support plain language. To some extent in the industry there is already a move towards it. There have been a few companies so far that have published their plain-language terms of service. Essentially the language is along the lines of saying "We're going to share your information with third-party companies.

Are you okay with that?"—using simple statements, simple language that people can read and understand very quickly. The companies that are doing this are getting a lot of praise from those around them. There's a lot of push to actually do this.

Beyond that, within the market research space we pride ourselves with the "do no harm" phrase. We know that a lot of people don't read those, don't understand them, and we take it upon ourselves to be a sort of overseer. We respect that not everybody knows or understands. We will look out for you on your behalf. When we see that something should be done in a certain way, even if it's technically legal, if we don't think it meets our higher ethical standards, then we'll make sure to do what we know is the right thing, even though it goes beyond checking the box that nobody has read.

One final point is that observational research, which is essentially what social media research is all about—looking at what people are saying, looking at what they're doing—has a long-standing tradition as a legitimate research method. Sociologists, anthropologists, psychologists have been doing this for more than a hundred years. It's a standard practice. It's becoming more and more popular now with social media—it's easier to do it and you can observe a lot more people doing it—but we still take pride in ensuring that what we do is following the "do no harm" methodology.

[*Translation*]

**The Chair:** Thank you. I am going to have to stop you there, unfortunately.

We now go to Mr. Andrews, for seven minutes.

[*English*]

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

I'm trying to get my head around something here this morning. I'm going to make a statement, and I want you to correct me if I'm wrong or clarify it.

Listening to you this morning, I'm getting the impression that there are two types of data that we're looking at. We have Facebook, Twitter, and the companies that actually own the data that is put into it by people and then they either resell it or they market it themselves.

Then what I think I heard you say this morning, Annie, is you guys observe data online. You're not actually in possession of it. From your perspective, and from the place you guys come today, you're looking at that data that's online. You're not actually talking about the data that is owned by the companies.

Is that a fair statement? I'm trying to compartmentalize this into two different things here and I don't know if I've done that.

**Ms. Annie Pettit:** We indeed collect that data, so what we see online we bring it in-house, so that we can measure the opinions, aggregate the opinions, and come to the research conclusion. So we do collect that data.

**Mr. Scott Andrews:** You collect that. So what you're advocating today is separate from what these companies do with their data. There are two distinctive types. Facebook could have its data on individuals and they can sell it, push it, and market it. You do it outside. Okay.

You mention that you don't go into a password, but most of these sites, the social media sites, have passwords. You have to access them. How do you get the data without accessing...? When you Google something, what comes up, comes up, and often you're linked to the site to go get it. So how do you square that circle?

• (1140)

**Ms. Annie Pettit:** There are two kinds of passwords. There is one kind where you must enter the password before you can actually enter the website and see anything at all. It is completely blind. You don't see anybody's names, photos, user IDs, comments, nothing, until you create a password and go inside. That is a large portion of Facebook and medical kinds of sites where patients talk to each other.

Then there are the other kinds of passwords that are simply there, so that I have my space and my friends see what I have written, and everyone can follow each other. We know that because there is a name associated with each comment. That's the second kind of password.

Those are searchable by whatever browser you want to use, the Googles, and that's the kind of data we collect—only the data that is physically viewable if you were to go online and not have your own password.

**Mr. Scott Andrews:** How many different social media companies are we talking about? We know the big ones, but how many are out there that would have to comply with all the privacy issues?

**Ms. Annie Pettit:** Strictly social media research companies—there are not a lot. Certainly, under 100 are social media research.

Then there are untold hundreds of other companies in the social media monitoring space. They're not members of any kind of research organization, no industry organizations, but they're doing similar kinds of things. They're counting, reading, and listening. Some of them are providing pieces of measurements, but they don't classify themselves as a market research company as mine is.

**Mr. Scott Andrews:** I'm going to come back to that, but here is the second part of my question. How many social media companies are there, like the Facebooks, the Twitters?

**Ms. Annie Pettit:** Thousands, millions? I do not have the exact number.

**Mr. Scott Andrews:** We all talk about the big ones, but how are we going to make something that's applicable to not only the big social media companies but the small social media companies...?

**Ms. Annie Pettit:** There are probably 100 new ones every single day.

**Mr. Scott Andrews:** Really?

**Ms. Annie Pettit:** Oh, for sure. There are the top 100 Facebooks, LinkedIns, and Twitters, but it goes far, far beyond that.

**Mr. Scott Andrews:** Back to the market companies. Near the end of your statement you talked about self-regulating. How do we as politicians trust people to self-regulate when there are so many of them out there? I'm sure there are good ones and bad ones, but how do you have faith that some sort of self-regulation will work?

**Mr. Brendan Wycks:** In the case of our association, I think the parliamentarians and legislatures can have faith and trust based on our track record over many years and the self-regulatory mechanisms we have in place. For example, we have a mechanism called the research registration system, under which companies go on our site and register the projects they have out with the public at any given point in time. That allows respondents across the country to phone in or by e-mail verify the legitimacy of the survey, because it has been registered with the self-regulatory association.

In the case of the social media companies, it's a difficult task, because they're so numerous and so varied and they cater to different sizes and types of audiences. Even for, say, an association within Canada, such as the Canadian Marketing Association, it would be a monumental task to bring all those types of companies into the tent and get them to agree to adhere to standards and proper self-regulation. I know there is a characterization out there now that social media marketing is like the wild west, because none of them belongs to self-regulatory associations.

**Mr. Scott Andrews:** Go ahead.

**Mr. Warren Everson:** I'll make a quick point here.

Self-regulation is a subject in its own right, but it is illegal to collect personal information and resell it in Canada without consent. So we're not relying on self-regulation to protect the privacy of Canadians: PIPEDA already bans that practice.

**Mr. Scott Andrews:** Any time you have this, how does the government or how does anybody police it? It must be very difficult to police, unless it's complaint-driven.

• (1145)

**Mr. Warren Everson:** Response to most crime in Canada is complaint-driven. We don't preauthorize transactions and so forth. You have to be robbed before you complain to the police, before they investigate the robbery.

I understand what you're saying, but I don't think the assumption should be that commerce shouldn't take place until an agent of the state has approved it. It has to be responsive to criminality.

**Mr. Scott Andrews:** That leads me to the question I had for you.

Do I have some time?

[*Translation*]

**The Chair:** No, I am sorry.

We now move to Mr. Calkins, for seven minutes.

[*English*]

**Mr. Blaine Calkins (Wetaskiwin, CPC):** Thank you very much, Chair.

Mr. Everson, thank you very much for coming today.

I saw you last week at committee. You're a man of many talents. You're able to come and talk about a wide breadth of issues on behalf of the chamber. It's much appreciated.

Of course, Mr. Wycks and Ms. Pettit, thank you very much for being here.

I have some concerns about the industry in general. I want to talk about something Michael Geist, who testified before our committee last week, said. He said the devil is in the defaults. I thought that was quite apropos. From my perspective, what I would like to see out of this is that the need to protect individual Canadians' privacy be balanced against the economic growth that you talked about, Mr. Everson.

I think that's key. I'm glad we have some semblance of self-regulation here and have an inward-looking organization like yours, which basically monitors how we're doing things and how we're conducting ourselves. I think that's a great thing. I believe we should only have government where necessary, not necessarily have government in all aspects of our lives. But I do think the government has a role to play here, and I'll be getting to that.

I'd like to talk about "the devil's in the defaults". I have young kids who have iPods and all these other kinds of devices. I do what I can as a parent to protect my children, to protect the integrity of our network in our house, but there's only so much that it's reasonable to do. I read through pages and pages of agreements—user agreements and so on. They're written in a language that frankly I don't think most lawyers could even understand, much less lay people. I'm surprised often, when I find out, that the default settings on most things that I accept an agreement to.... They sometimes frighten me in the degree to which I've allowed my personal information to be shared.

I would like to ask you, Mr. Everson, do you think we have an appropriate balance right now? You were fairly complimentary to PIPEDA. Do you think we have enough protection from the perspective of protecting people's information right up front, right at the very first opportunity, by the use of default settings as to what can be shared and what can't be shared?

To Mr. Wycks and Ms. Pettit, from a self-regulatory perspective, do you think the groups that you represent—the organizations, your

clients, the people you study, the people you do work on behalf of—are using defaults appropriately?

**Mr. Warren Everson:** Thank you very much. It's nice to see you again.

Mr. Calkins is getting close to his maximum safe exposure to Warren Everson this week. You want to be cautious about that.

That's a really big mouthful of a question, as you know. I think society will use a defence in depth with regard to privacy. That defence will include a proper understanding of what the consent is. I certainly support the committee in the tone of your questions concerning frustration about consent being hard to follow and hard to understand. I don't suppose the suppliers of the service necessarily take much joy in it either.

I think the caution of the consumer can't be ignored. My children are much more concerned about Internet privacy than I am, because they have been lectured to about it so much and can cite off all the rules that exist for the social media they're employing. I don't know whether they represent any standard or not, but they are certainly not unconscious of the issue; they are suspicious.

Madam Borg started with asking whether there is a lack of trust. There is a lack of trust, and it's probably a darned healthy thing that it exists there.

We have seen in the last couple of years some pretty significant changes to privacy in the big offerings. Facebook has upgraded its privacy standards, and that's an ongoing debate. You can hardly pick up a newspaper without seeing discussion about it. I note that Google handles people who identify themselves as young consumers differently, as to how much information is available in their social chat services. I became aware not long ago of a service called Hangout, where people can go and hang out. When a stranger enters that enclave, everyone is notified, and if the stranger does not properly identify, the site closes, so they would have to reassemble it. There are all kinds of technical security and privacy services that have been invented by the technical side of the business, conscious of consumer concern.

I'm just going to say one more thing. As you proceed in your hearings, obviously you're going to want to know exactly what the law currently makes illegal and how often it has been employed by people. It's my contention that the law is not bad in Canada. Probably public awareness is quite low as to exactly what recourse exists.

•(1150)

**Ms. Annie Pettit:** These days, as Warren was saying, kids are being raised with privacy in the digital age. From the youngest age, this is a normal everyday conversation, whereas for many of us it didn't even come about until, let's say, 10 years ago. So this is brand-new information; it's completely different from how we were raised, and we're still wrapping our heads around it. Kids are far more aware of it; it's just normal for them. They know what is good and what's bad in terms of wanting or needing privacy. That's why they have more opinions on it than a lot of us have.

In terms of our people using defaults appropriately, I think a lot of industry is doing just what we're talking about here, its own self-regulation. When somebody changes a default setting, as in the case of Facebook, everyone is in an uproar if they don't like it, and there are some quick work-arounds to make adjustments to it. It's happening in one website after another website: people continue to speak up when they don't like what the default setting is, there's a whole bunch of discussion around it, and then tweaks are made.

So I think there is a lot of self-regulation going on in the industry, and it will only get more and more and better and better as people become more familiar with how it should be and how they want it to be.

**Mr. Blaine Calkins:** My last question is about the differentiation between data and information. When information is collected about me as a user on the site, my personal information is there, if I happen to be creating an account, for example, but there are also traces of my user information, the sites I go to, things that I may visit, my interests, my hobbies. They can glean this kind of information.

When it comes to reselling this information or data, are you confident, from an industry self-regulation perspective, and comfortable with the fact that enough de-identification of some of the personal things is actually happening? If they happen to know what age group I'm in and what I happen to be looking at or shopping for on the Internet, that's one thing; if they know my name, address where I live, and what I'm shopping for on the Internet, that's a completely different thing.

Are you satisfied that there's enough de-identification? Do we have enough legislative framework around the de-identification of the information that's being resold between the data collector and those who might be interested in it?

**Ms. Annie Pettit:** This is already part of what the MRIA code looks at. All information must be de-personalized. This is the exact same thing we are doing within the social media space. Our ethical standards are exactly the same as they would be for survey research. Names are not published in research reports; there are no user names, photos, e-mail addresses, physical addresses. That kind of information is not appropriate, and we do not allow that sort of information to be published in final reports.

[*Translation*]

**The Chair:** Thank you. I am going to have to stop you there because Mr. Calkins' time is up.

We now start the question and answer period where each round is five minutes.

Your turn, Mr. Angus.

[*English*]

**Mr. Charlie Angus (Timmins—James Bay, NDP):** Thank you for a fascinating discussion.

Mr. Everson, I was a two-time board director of the Chamber of Commerce. At the time I was on the board, I was representing a small northern Ontario media company, and we were looking at the possibility of where we could move in terms of digital culture. I agree with you; I think the opportunities have exploded since, and even as we were watching it develop. I think Canadians are well positioned to take advantage of this. We have to encourage that. I think it's part of what our work at this committee is to do, to find out how we build the climate that allows that kind of innovation.

The issue here is about consumer confidence and the threat of data breach. Those are the issues I think we need to look at. When we ran our magazine, our database was our commodity. That was the value of our work. It's what allowed us to do value-added sales. We had many groups offer to buy this data from us, but it was an issue of trust with the people who purchased our products. They were our subscribers. We kept that.

If someone had wanted to breach that data, they would have actually had to break into the house, steal the computer, and then they would have gotten it. Now, however, in terms of what's online, it seems that when we have this discussion about informed consent, we're talking about an understanding of an old style of business model—you click on something, and it's about a commercial relationship or a sharing of information—but in the age of big data, it's a question of function creep. It's so easy to access data. You can access data through algorithms just casually. This is the concern.

My concern is about a breach of consumer confidence. For example, if I'm at a café and I use their WiFi, there's an agreement. I sign that yes, I'll abide by the rules. But we had the case with Google Street View going by. They were gathering WiFi hotspots, and that was a good business model for them. But there was the whole matter of load data that was collected as well, which could include e-mails, medical records.

I didn't sign on for that in giving initial informed consent. The people who gathered that data might not have even been looking for it, but the data is gathered up.

So, Mr. Everson, how do you see establishing some kind of framework to ensure that consumers have confidence, that the model is able to develop, and above all, that data breaches—because they would affect people's security—don't happen?

• (1155)

**Mr. Warren Everson:** Thank you for the question. It's pretty sweeping.

I guess the first thing I would urge the committee to do is to exactly understand how PIPEDA currently works, because some of what you're describing could be illegal in the existing act. I know you're going to hear from various carriers about specific high-profile incidents, such as ones you described.

I don't know of a more challenging issue for the committee than addressing the expectation of privacy in an online environment. I don't want to patronize anyone, but when I was growing up in Lancaster, Ontario, we had a general store. When you went into the general store, the vendor knew you and knew your buying habits. If you dramatically changed your buying habits, they would notice that, or perhaps they would say, "Oh, you're here, and I know you like this kind of stuff, so I got a new one. Do you want to have a look at it?"

We didn't consider that an unwarranted intrusion into our privacy. But when a company now contacts me and says, "I know you're interested in canoeing", I would say, "Oh, how did you know that?" They know it because they have access to a lot of vendor sites in canoeing.

I think you've identified correctly the challenges. One is of consumer confidence. Consumer confidence goes both ways. We want to trust that we have enough privacy to do business online. We also want to trust that the company is using the information we have to prevent exactly the opposite side of your equation, which is the data breach.

I got a call last year asking, did I buy \$12,000 worth of drywall on my credit card yesterday. No, I did not. I was very glad that they had my personal information and were able to contact me abruptly and stop that. So fraud protection is a very significant part of the online world as well. I don't know that you're going to find an exactly easy balance between those two pressures.

**Mr. Charlie Angus:** Mr. Wycks, I'm interested in this issue of—  
[Translation]

**The Chair:** You can ask a quick question.

[English]

**Mr. Charlie Angus:** —self-regulation and the support for administrative monetary penalties. Industry needs to be able to regulate itself if it's going to succeed, but there are going to be a few bad actors out there, and bad actors will damage your business model. So you support the idea of saying, for those few bad actors, that you support the Information and Privacy Commissioner's being able to hold them to account so that the rest of the industry can continue to develop. Is that your position?

**Mr. Brendan Wycks:** Yes, for those who violate PIPEDA.

**Mr. Charlie Angus:** Okay. Thank you.

[Translation]

**The Chair:** Thank you very much, Mr. Angus.

It is now Mr. Dreeshen's turn.

• (1200)

[English]

**Mr. Earl Dreeshen (Red Deer, CPC):** Thank you very much, Mr. Chair.

Thanks to you folks for being here today.

First of all, Mr. Everson, I want to commend the chambers of commerce, because they do some amazing work. You're able to get out and talk to businesses throughout the country and bring in information. Many of us depend on the information that you're able to present.

One of the things you mentioned when you were talking about PIPEDA was that the Canadian rules work and they're still relevant. Of course, this is what we're trying to do, and we're trying to take a look at some of the other things. We know there are critics out there, of course, and people who would like to see some significant changes, but in your commentary you talked about us not putting in excessive regulations for fear of losing jobs.

I'm just wondering if you could expand upon that. Also, of course, as this discussion is on social media, I'd hate to be accused of just having a time-killing question, so if you could answer that quickly, I do have a couple of others.

**Mr. Warren Everson:** I'll try not to be too long. I thank you for your comments about the chamber.

I think it's very apparent that PIPEDA was designed by people who understood that they didn't understand, and that they would not know where the technologies were going to go and where the offerings in the marketplace were going to go. They were wise enough to say that they couldn't be extremely doctrinaire as to how the law would apply and that they were going to have to see....

One of the important functions there was to establish the commissioner as an ombudsperson and not a police force. I'm always a little uncomfortable with people who want to make the officers of Parliament into regulators. They're not. It's a unique role they have.

If you want to install more police powers, you have to take it out of the parliamentary officers and into one of the departments of government, and I do think that you already have recourse in the law for a lot of the concerns that are expressed.

**Mr. Earl Dreeshen:** Thank you.

Ms. Pettit, you were talking about how you, in your organization and research, are not selling information, but is that evident to respondents upon your first contact? When you are talking to different groups or when you are going into different sites, it is evident to everyone that this is your role?

**Ms. Annie Pettit:** We do not enter sites for the purposes of engaging or communicating with people. We strictly observe—nothing more. That is what the essence of social media research is all about: listening only. There's no engagement.

**Mr. Earl Dreeshen:** Okay, but when you're researching information, then, from various companies, if you believe they're not acting appropriately or clearly, do you have any associative ability to interact with those companies to encourage them to change their practices? When you observe what is happening online and you see something that you have some concern about, do you have any clout that you can use in order to make them aware that they're off...?

**Ms. Annie Pettit:** In most cases they're actually very eager to know if something is happening that they should be made aware of. So when that does happen, they're on top of it, because they don't like it either, whatever that issue may be.

**Mr. Earl Dreeshen:** Okay. Thanks.

Again, with this particular study, do you have any suggestions about some specific aspects of privacy and social media that we should be looking at?

**Ms. Annie Pettit:** A lot of it comes down to respecting the different ways of communicating that people have. You were mentioning engagement. There's a lot of discussion on what is or isn't appropriate.

In terms of social media research, where we are simply listening, we don't engage. There needs to be some understanding that not everyone wants to engage, and that if they do, it needs to be up front, with permission. As we normally would do with traditional market research standards, there needs to be permission before you pursue anything any further.

**Mr. Earl Dreeshen:** Mr. Everson, on the same point, is there anything specific that you would like to see us studying when it comes to privacy and social media?

**Mr. Warren Everson:** I tend to be on the booster side. I think it's a fascinating industry, and I think Canada is doing extremely well. The kinds of services that are available to me now are tremendous, even just in the last few years.

I tend to think the committee's approach should be this: prove to me there's something wrong with our current form before I make any changes. I often hear comments about complexity and clarity for consumers. I believe the whole system is based on an informed consent. Around those questions I think you're in a very important area. It's not obvious what the simple solutions are. I think consent in all of the different constituencies of the public is extremely critical. That is the place you're going to end up spending much of your time.

• (1205)

[Translation]

**The Chair:** Your time is up, Mr. Dreeshen.

Mr. Boulerice, you have five minutes.

**Mr. Alexandre Boulerice (Rosemont—La Petite-Patrie, NDP):** Thank you, Mr. Chair.

My thanks to witnesses for sharing with us their opinions and practices and for giving us their vision of the issues involved in protecting people's privacy.

I was really struck by your presentations. I noticed that the level of concern was quite different from what we heard from witnesses last week. We had university researchers here to see us and we asked them questions. They were more concerned than you seem to be about the protection of privacy. We got the impression that Canada was dragging its heels little and was falling behind in terms of legislation protecting the privacy and the personal information of Canadians and Quebecers.

Do you feel that the existing legislation is sufficient? Does it guarantee a balance between economic development, the protection of jobs and the protection of privacy? Is our country in a good position in that regard or are we behind others?

[English]

**Mr. Warren Everson:** So far, I would say Canada is doing very well. I mentioned the resolution of the chambers of commerce of Canada last year, which I will table with the committee, that said exactly that: there's a balance, but thus far PIPEDA seems to be meeting the needs of society.

I would say that in your position you should have people prove to you that there's a very serious problem that needs to be addressed before making dramatic changes. That's not in any way to say that the population doesn't need to be reminded constantly, especially as services evolve and change. It's their responsibility to watch out for their privacy, and they should take privacy seriously since this information is going to last for a long, long time.

**Mr. Brendan Wycks:** Our association is on the official record, through the most recent PIPEDA review, as supporting some greater powers for the Office of the Privacy Commissioner: mandatory breach notification and greater enforcement powers. We think PIPEDA, which is over a decade old now, has served the country well. It has put Canada in a good position. It just needs a few tweaks to bring it into the modern age.

[Translation]

**Mr. Alexandre Boulerice:** Thank you.

Don't get me wrong; I'm a big fan of social media. I use them; I'm not an addict, but it's close. For a politician these days, social media are an indispensable tool for reaching people and making them aware of various issues.

But still, social media's business model is based on the ability to gather information. Information is power, as they say. Some large organizations have a ton of information and data on millions of people. If information is power, couldn't some private organizations and large companies become too powerful at some point? Could that be a danger? Are people right to be concerned?

[English]

**Mr. Warren Everson:** I guess my perception is that the large companies have demonstrated quite a bit of sensitivity to concerns. They are aware that consumer concern about privacy is one of their most significant business issues.

You're going to see, over the next few months, an interesting discussion about a technology called "do not track", which is a service that you can install. The different providers are all approaching this in a different way. One provider is going to make it the default; one provider is not; one hasn't decided yet. They're struggling with how to meet customer demand for privacy while simultaneously knowing that you and I and everyone else appreciate, without thinking about, a lot of the services we are provided.

I'm very glad that the credit card company was able to spot that it was unusual for me to buy \$12,000 worth of drywall on a given afternoon. It didn't occur to me that it was a breach of my privacy, though I guess you could make that case.

I would address, instead, that the committee should not be preoccupied always with the monster companies at the top of the food chain. First of all, they won't always be at the top of the food chain. The next major innovation in the business might be fermenting away in the lower basement of someone's apartment right now.

Also, it's very difficult to make regulations in the environment of saying, "Well, this is a huge company and they can afford all this. They can afford notification and constant checking." That can be a considerable constraint on smaller companies that are trying to evolve in the marketplace and cannot do that.

So it's very challenging for the committee to say that there's a solution that fits all.

• (1210)

[Translation]

**The Chair:** Thank you. Unfortunately, your time is up, Mr. Boulterice.

Do the other witnesses want to answer?

[English]

**Mr. Brendan Wycks:** As to whether the size of some of these large social media companies gives them too much power, I would just respond that, yes, data is power, and they are quite powerful, but that power is somewhat tenuous. They are vulnerable, because the power is rooted in consumers' confidence in them. If there were a major breach or some kind of thing that caused harm to a group of citizens, or even down to a single individual, and they suffered a lot of negative publicity and damage to their corporate reputation, I think they would be dramatically diminished quite quickly.

[Translation]

**The Chair:** Thank you.

Mrs. Davidson now has the floor for five minutes.

[English]

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

Thank you very much to our witnesses for being with us this afternoon. As you can see, this is a subject that the committee is finding extremely interesting. It's certainly more involved the more people we hear from, so it's great to hear from the experts and those who certainly understand it a lot better than I do.

There have been a lot of different comments made here today, and I think I would like to ask Ms. Pettit the first question.

I know we talk about social media as being one of the greatest tools there is for researchers, and that it will become more important as we move forward and social media becomes much more the norm in many more circles than it is today. I agree with that, and I think we need to move forward, but I think we need to move forward in a way that is responsible and that is safe. I think that's the crux of what we're trying to determine.

I understand that you certainly do market research and that you don't sell articles, but as has been stated, the people you sell your research to do sell articles. We need to make sure the public is protected.

Now, one of the statements that I thought you made was that you weren't interested in seeing stricter rules that would hamper your collecting information in an "ethical" way, as you describe it, that what you're doing now you're doing in an ethical way, and that because of the rules that are in place, you're able to do that.

If the rules are changed, I think you indicated—or intimated, at any rate—that it would force you to collect information in another way that may not be quite as ethical. Could you...?

By the look on your face, I guess you didn't quite say that. Please elaborate on that and straighten me out on this issue.

**Ms. Annie Pettit:** Sure.

My intention, by my earlier remark, was to say that if I can't do it ethically, then I personally, in market research in Canada, won't be able to do the work.

**Mrs. Patricia Davidson:** So nobody will be able to do—

**Ms. Annie Pettit:** In Canada—

**Mrs. Patricia Davidson:** Okay.

**Ms. Annie Pettit:** But what will happen is that for other countries where they don't have the kinds of ethical standards that we do, off they go, they can do whatever they want, and their work will potentially harm, will be unethical, and will not be in the best service of Canadians, as it would have been if the work had been done by Canadians for Canadians.

**Mrs. Patricia Davidson:** Are there comparable rules now that are making it an even playing field, or are there still some discrepancies?

**Ms. Annie Pettit:** Well, there's ESOMAR in Europe, and there are CASRO and MRA in the U.S. I was on the committees for all of those social media research committees. We're all on board and all in the same place—which is that this kind of work needs to be done ethically—and we're all in the same place on what that ethical standard is and should be. A lot of other countries are looking towards those standards in terms of developing their own country-specific standards.

•(1215)

**Mrs. Patricia Davidson:** So do you think we're continuing to be a leader, then, and not falling behind when it comes to the protection of personal privacy?

**Ms. Annie Pettit:** Currently I think we can do that. We just need to make sure that PIPEDA allows us to continue doing that, so that the work can stay in Canada and we can do it in an ethical way.

**Mrs. Patricia Davidson:** So what are some of the things, then, that you would not want to see? What are some of the things that would prohibit you from continuing in your ethical practices?

**Ms. Annie Pettit:** Well, there are some definitions in terms of what public data is. If what people write on Twitter or on some social forums is determined to be private data, then basically this work cannot take place in Canada, and social media research will be moved to other countries.

**Mrs. Patricia Davidson:** Okay. Thank you.

Mr. Everson, in one of your replies, I believe, or one of your explanations, you talked about privacy safeguards for young people. I forget what kind of site you said it was, but you said that if somebody comes on who's a stranger to that site, it will shut down if they don't identify properly. What do you mean by "identify properly"? Who determines that? Also, how can you be assured that what someone is saying when they're identifying themselves is in fact anywhere near the truth? Can they not just make up anything they want and self-identify?

**Mr. Warren Everson:** In that particular case, I was citing a service called Hangout, which I think Google offers, which is actually a video conferencing facility. The users themselves determine who's in the club, and they hang out together. When someone else enters, the machine tells them that someone else has entered. If they can't verify who the new entrant is, the service shuts down. I mention it only as an illustration of the ingenuity of people who are trying to provide the service and also provide the protection.

I guess you'll hear from witnesses from all of these companies. I don't think anybody can deny that they have a high sensitivity to their names being tossed about in the context of carelessness about people's privacy, so my concern is not that the best operators do not want to do what's right and do what they can for their consumers. That's why I say that it's quite difficult to invent user rules that are one-size-fits-all rules.

One of the reasons why I've appreciated PIPEDA is that it causes the officers of Canada to examine every situation sort of uniquely against a measure of reasonableness, as opposed to saying that they have a defined lockdown and everybody has to fit this picture even though the technology is rendering it moot.

[*Translation*]

**The Chair:** Thank you. Unfortunately, your time is up, Mrs. Davidson.

Ms. Borg now has the floor for five minutes.

**Ms. Charmaine Borg:** Thank you.

I would like to go back to a couple of things. I wrote these questions down while you were answering others.

You said that your organization collects data. Do you subsequently destroy it? How do you do that?

[*English*]

**Ms. Annie Pettit:** It often happens like it does with traditional market research. It might be a tracking study that takes place every week or every month for the next year, two years, or three years, so we can track trends over time. In that case, the research data is held until that particular project is finished. If it's finished next year or the year after, then that project is closed and we no longer require that data.

In the meantime, another client may have picked up on that same type of project. I mentioned Nike earlier. Let's say that one client is using Nike data and they finish on one date. Another client may start using the Nike data and continue on. For a popular brand, that stretch of data may be continually closed and opened, closed and opened—it might be ongoing.

For a smaller research project, a one-time project, we use the data, and if nobody else is going to use it, then we no longer require it and we can get rid of it.

[*Translation*]

**Ms. Charmaine Borg:** Mr. Everson, you mentioned the "do not track" service that has just started up in the United States. It is really quite recent.

I find it interesting because the initiative comes from the companies. I know that the Federal Trade Commission plays a role in it too. Could you tell us more about it? Is it a model that we should encourage in Canada?

•(1220)

[*English*]

**Mr. Warren Everson:** I think the committee is going to want people who are more technically profound than I am to answer this question. "Do not track" is a service that would be in a browser, which would prevent the lodging of cookies in your computer. Currently, when you identify yourself and you indicate your language of choice, and other things that you want the service to know, it will register that and lodge a cookie in your computer so that every time it comes to you, it says, "Oh yes, this is algorithm such-and-such, and these are the preferences."



There can be a whole series of things that are pre-approved. “Do not track” would block the registering of cookies, so you would be a fresh face every time the website was opened or the service came to you, if it was a social service.

The different offerings are looking at that differently. I believe that one of the biggest recently announced that they would register that as a default setting, and a consumer would have to disable it in order to receive cookies that might facilitate transactions. Another big operator is currently indicating that they're not certain they want to do that, because they think the consumer prefers to have more facilitated service. So it's a really interesting debate.

To your point, there's a reason these companies are doing it and states are not ordering them to do it, and that has to do with the sensitivities around privacy. It's a healthy discussion to be having, and it's nice that they can invent a technology like this.

I'm not necessarily as concerned about it. I read the consent provisions carefully, so that's my defence.

[*Translation*]

**Ms. Charmaine Borg:** Thank you.

Some experts have told us that the technology sometimes does not make sure that information is completely destroyed. In fact, the technology sometimes gathers data without the company knowing. Are there any members of your organization who are concerned about that or who have had the problem?

[*English*]

**Mr. Warren Everson:** I haven't heard of any of those concerns.

I can well imagine how that would occur, but if they're inadvertently collecting, then they're probably not turning around and abusing anybody's privacy by reselling or using that data. I haven't had that one.

[*Translation*]

**Ms. Charmaine Borg:** My next question goes to Ms. Pettit and Mr. Wycks.

We understand that you just observe. Do you observe people's online habits? Because of the cookies, do you know the websites that people go to when they buy shoes, for example? How about a 16-year-old looking for clothes? Do you observe that sort of thing too?

[*English*]

**Ms. Annie Pettit:** I don't have enough information to comment on that. I don't know.

[*Translation*]

**Ms. Charmaine Borg:** Are you going to monitor online behaviour?

[*English*]

**Ms. Annie Pettit:** We monitor opinions online. I'm sure some companies monitor behaviours online, but I'm not familiar with any trends. I don't have any information to share.

**Mr. Brendan Wycks:** I'm aware of a study that is done, I think annually, by a major research company that happens to be a member of ours: TNS Canadian Facts. It monitors Canadians' attitudes towards things like online behavioural advertising, so the tracking

that is done through cookies on their computers, and then the custom ads that are served up to them, and their like and dislike for that sort of thing.

I saw a study along those lines that is about a year old now. So our industry is monitoring that sort of thing.

[*Translation*]

**The Chair:** Thank you.

Mr. Butt, you can make one last comment.

[*English*]

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

Thank you very much for being here.

My first question probably would be for the Chamber of Commerce. When you are surveying your members or finding trends in what your members are looking at and in their use of social media, etc., obviously for doing business, for selling their products or for interacting with customers or whatever, are you finding that is becoming the largest trend for how companies are getting new customers and new markets? In marketing their products, are they shifting from traditional ways of contacting customers and moving more along this line, either through e-commerce opportunities, by having customers directly ordering product and services through their websites, etc.? Is that very much becoming a bigger and bigger trend as time goes on for Canadian businesses?

• (1225)

**Mr. Warren Everson:** It is absolutely, and moving to an online environment must be one of the biggest trends ever in Canadian businesses.

**Mr. Brad Butt:** I ran an association, too, before I became a member of Parliament, and it was an association for owners of apartment buildings. Of course, landlords have to keep personal information on their tenants and employees and others, and we found there was a lot more renting being done online, with people providing personal information about themselves as prospective tenants for renting apartments.

We really struggled with PIPEDA and what our responsibilities were. As an association, we actually went out and hired legal expertise to draft a standard privacy policy, to draft some regulations, to draft some wording, although it was very legalese wording. I wish it had been simpler, for people to understand so that they could actually place it on their websites and they could actually have it within their companies, so that our members were absolutely doing their very best—

**Mr. Merv Tweed (Brandon—Souris, CPC):** You can't do that.

On a point of order, you don't share information with the media on an in camera meeting. I'm sorry, you just don't do that.

**An hon. member:** Well, this isn't in camera.

**Mr. Merv Tweed:** The note you got is in camera. Mr. Chair—

**An hon. member:** We're not in camera, Merv.

**Mr. Merv Tweed:** You don't share in camera information with the media. Scott, think about it.

Shame on Kady for even walking up and asking for it. She knows better than that too.

Mr. Chair, I ask you to rule on that. This is not the way a committee is run.

[*Translation*]

**The Chair:** Certainly, at the moment, the meeting is not in camera. Like you, I also understand that the report is still in draft stage. So it would not be appropriate to make it available to the media or to anyone else who is not a member of the committee. The committee would greatly appreciate it if the copy of this draft report, which is not yet a public document, could be returned, if in fact it was given out. Okay, I am told that the copy was not given out.

So we can continue.

[*English*]

**An hon. member:** What was that, sir? What did you just say?

**Mr. Merv Tweed:** I said you have a sick relationship with the media, sharing in camera information.

[*Translation*]

**The Chair:** We will suspend the meeting for a few minutes.

My thanks to the witnesses for coming here today.

We will come back to committee business a little later. I am sorry, Mr. Butt, but we are going to have to suspend the meeting.

- \_\_\_\_\_ (Pause) \_\_\_\_\_
- 
- (1230)

**The Chair:** We now resume the meeting. We are discussing committee business. We have a number of items on the agenda, including the budget for the committee trip to Washington.

Mr. Del Mastro, do you want to say something?

[*English*]

**Mr. Dean Del Mastro:** Are we in camera, Mr. Chairman?

[*Translation*]

**The Chair:** No.

[*English*]

**Mr. Dean Del Mastro:** I would move that the committee go in camera for consideration of committee business.

[*Translation*]

**The Chair:** Mr. Del Mastro moves that the committee meet in camera. That motion is not debatable. A recorded vote has been requested.

(Motion agreed to: yeas 7, nays 4. ([See *Minutes of Proceedings*]))

[*Proceedings continue in camera*]







**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>