HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 050 • 1st SESSION • 41st PARLIAMENT

EVIDENCE

Tuesday, October 16, 2012

Chair

Mr. Pierre-Luc Dusseault

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, October 16, 2012

● (1530)

[*Translation*]

The Chair (Mr. Pierre-Luc Dusseault (Sherbrooke, NDP)): Good afternoon, everyone. As it is 3:30 p.m., we will begin.

Before we get started, I want to let you know that the bell will probably ring for votes at 5:15 p.m. So we will have to end the meeting 15 minutes early.

I want to thank the three witnesses with us—Mr. Péladeau, Mr. Elder, as well as Mr. Zushman, from Winnipeg, who is joining us by videoconference.

Without further ado, we will begin with a 10-minute presentation by each witness. As usual, that will be followed by a question period for committee members. I yield the floor to Mr. Péladeau. You have 10 minutes for your presentation.

Mr. Pierrôt Péladeau (Researcher and Consultant, Social Assessment of Information Systems, As an Individual): Thank you, Mr. Chair, ladies and gentlemen members of the committee.

As I have read previous testimonies, I am submitting eight comments on the issues that have not yet been addressed.

The first comment is that social media do not constitute a commercial sector. Social media are rather made up of a variety of applications that make it possible to create and exchange content used not only by a few well-known specialized companies, but also by all kinds of commercial companies, public organizations, associations, employers, schools, universities and even hospitals, which are currently developing social media applications.

Social media are not only used by people. They are also used by machines. For instance, police officers, social workers and people working in shelters now have to explain to the adults and children under their protection that their computers, tablets, telephones and cameras automatically send out information that helps locate them.

In short, social media constitute an environment. Therefore, the solution cannot be based on a sector-by-sector approach that applies to certain companies—or even to the whole private sector—but rather on a universal approach that would also apply, to an extent, to the makers of certain machines that produce such information. We are now living in an era called the Internet of things.

Second, the transparency of social medium processes is not only important for operators so that they can meet their legal obligations, for individuals so that their rights are respected or for the commission so that it can do its work. That transparency is also important so that third-party organizations can meet their own obligations.

I will give you a very simple little example. The Sleeman Brewery launched the Break into Alcatraz contest, which had to be entered by accessing a Facebook page. However, the operation of that Facebook page was breaking the official contest rules. So Sleeman was more or less in violation of laws on draws and promotional contests and the personal information protection legislation. I have two points to raise with regard to that.

The application required individuals to be Facebook members in order to enter the contest, but that was not listed in the eligibility conditions. Contest rules stated that no personal information would be transmitted to Facebook, but the application required people to click on the “Like” button on that page and, therefore, to produce and disseminate members' personal information.

The most likely explanation in a case like this one is that the professionals hired by Sleeman did not understand the Facebook processes, or how Sleeman's application process was tied to it. That brings me to the third comment.

The user-friendliness of social media gives a false impression of transparency. To illustrate, I refer you to the first figure distributed to you. The common perception is that a tweet has 140 characters. That is false, as you will see in the figures. A tweet has several hundred characters, making up about 30 different personal information fields. The same goes for the process. Users think they can see what their information goes through. In reality, the application is sort of like a black box where we can only see what the operator shows us.

Fourth, the wording of consumer contracts, conditions of use and statements regarding the use of personal information is not appropriate for explaining the processes involved. I want to point out that the first pieces of legislation for protecting personal information were adopted in the 1970s. So they were developed in the 1960s. At that time, this area was dominated by public or private bureaucracies where officials ensured that the information produced on an individual was compatible both with the internal organization processes and the individual's situation.

That challenge is called information pragmatism. I am now referring to the second figure, which sets out the factors that could determine the selection of good information for obtaining good results. I have a very simple example regarding that.

● (1535)

School admission and enrolment in a school year are two different processes requiring the identification of the mother, in both cases, unless we are not talking about the same person. The school secretary ensures that the right person is described. As part of the admission process, the person in the civil register is identified to distinguish among the little Tremblays, Smiths or Nguyens, while the enrolment process identifies the person who takes care of the child on a daily basis. So we may not be talking about the same person.

In the classic bureaucratic context, general implementation texts were sufficient because organizations had hundreds of officials who ensured mediation between the individual's reality and the organization processes. Today, millions of individuals are asked to manage processes on their own, and that's practical only on these two conditions:

1) that the individual obtain timely and specific explanations on the exact process they are undertaking;

2) that those explanations be comprehensible—including for children, technophobes or half the Canadian adults with low literacy levels.

Here, however, applications can be the solution because they are interactive and provided in multimedia. I want to go back to the Valerie Steeves example. On May 29, if the system has profiled me as a 16-year-old Vancouver teenager and listed the relevant interests of that profile, why would it not display that profile right away along with what exactly it is used for and by whom? That would help me adjust the parameters so that the system would be better able to meet my expectations and needs, somewhat like it is laid out in the figure I referred to earlier. This is not about revealing the industrial secret of the profiling algorithm, but rather about establishing a dialogue that will elaborate the relationship, and perhaps even the algorithm at the same time.

Here is my fifth comment. Even though personal information protection legislation has emerged largely in response to a risk of totalitarianism, and they remain a prerequisite to respecting personal rights, which are often guaranteed—for instance when it comes to issues related to child consent—those laws are nevertheless basically only an expression of principles that have to do with effective information management. I have participated in their implementation in over 500 organizations—both large and small—across all sectors. However, once the management was streamlined, the law was de facto respected. In addition, costs were reduced and processes enhanced.

Here is my sixth comment. The Canadian legislative model in terms of personal information protection basically covers only three logical and critical phases—production, conservation and communication of information. It is much less apt at covering the processing phase and the phase that consists in concluding the process that often leads to a decision. However, the processes cannot be explained adequately to users who deal with administration on their own without making all the phases transparent. As much as that individual empowerment is impossible without this understanding, the democratic dialogue among user communities, on the one hand, and developers and operators, on the other hand, is impossible without that transparency.

Here is my seventh comment. If the improvement of the Canadian legislative model continues through management principles applied at the level of logical phases rather than through the imposing of specific procedures, those standards could endure despite technological changes and be more easily accepted by operators.

However—and I am getting to the eighth and final comment—the way personal information protection legislation is organized is based on the ultimate purpose rule, or the principle whereby a predefined relationship with the individual is established.

Consequently, companies that have no clear business model or that favour the approach according to which they should generate any kind of information, as they will always find a way to use it, will never be able to accept any kind of legislation straight away, since the two logical approaches are contradictory.

● (1540)

In such cases, it is clear that those types of stakeholders can only be dealt with by clearly setting out the values and principles that are given force of law and by setting out powers to issue orders, as well as a substantial criminal sanction system that would help enforce the law.

So there you have the eight comments I thought I could add to the debate so far. Obviously, I am available to answer any questions you may have.

The Chair: Thank you, Mr. Péladeau.

I now yield the floor to Mr. Elder, from the Canadian Marketing Association.

Mr. Elder, you have 10 minutes.

[*English*]

Mr. David Elder (Special Digital Privacy Counsel, Canadian Marketing Association): Thank you very much.

Good afternoon, Mr. Chair and honourable members. My name is David Elder and I am a communications and privacy lawyer with Stikeman Elliott here in Ottawa. I also act as special digital privacy counsel to the Canadian Marketing Association, and it is in this role that I appear before you today.

The Canadian Marketing Association, or CMA, is the largest marketing and advertising association in Canada with 800 corporate members, embracing Canada's major business sectors and all marketing disciplines, channels, and technologies. CMA programs help shape the future of marketing in Canada by demonstrating the strategic role of marketing as a key driver of business success. The association's members make a significant contribution to the economy through the sale of goods and services, investments in media and new marketing technologies and employment for Canadians. Against this backdrop, the Canadian Marketing Association is the national voice for the Canadian marketing community, with the CMA's advocacy efforts designed to create an environment in which ethical marketing can succeed.

On behalf of the CMA, I would like to thank you for the invitation to appear before you as you consider the privacy issues arising in the evolving environment of social media. This afternoon I propose to address industry practices generally with respect to privacy issues that may arise with social media, focusing on the CMA codes and guidelines, in particular. However, as a representative of an industry association, I will refrain from discussing the policies and activities of any particular organization or company.

The roots of the CMA's involvement with the development of private sector privacy legislation and policy run very deep indeed, as it has been at the forefront of the Canadian privacy landscape for many years.

In 1995 the association was the first business association to call for national privacy legislation in order to establish basic principles for the protection of personal information. And it was one of the original members of the Canadian Standards Association's technical committee that developed the 10 CSA privacy principles.

Later, the CMA publicly supported the Personal Information Protection and Electronic Documents Act when it was introduced by the government. Association members were strong advocates for a law that would provide clear direction on how personal information could be collected, used, and disclosed, while at the same time retaining sufficient flexibility to enable businesses to take advantage of new and emerging technologies and to help grow the Canadian economy.

The CMA continues to believe strongly that this delicate legislative balance between individual interests and business needs produces significant benefits for both consumers and for information-based marketers, who comprise an increasingly significant sector of the Canadian economy.

Moreover, after the passage of PIPEDA, the CMA continued to be an active participant in the ongoing public policy debate concerning Canadian privacy law and its implementation. For example, several years ago the CMA proposed that the Privacy Commissioner of Canada initiate consultations with interested stakeholders with a view to developing breach notification guidelines, even in the absence of a statutory notification requirement. This consultation resulted in the issuance, in 2007, by the OPC of guidelines entitled, “Key Steps for Organizations in Responding to Privacy Breaches”.

Over and above its interest and involvement in legislative and public policy approaches to privacy, the CMA has long emphasized that marketers themselves have a responsibility to implement responsible and transparent personal information management practices, and they have an important role to play in promoting such practices.

In this regard, since the early 1990s the association has had a mandatory code of ethics and standards of practice, a self-regulatory code that provides CMA members, and marketers generally, with a comprehensive set of best practices for ethical marketing.

In 1993 the CMA was the first major private sector organization to publish and make compulsory a comprehensive privacy code governing members' activities, which is today structured to reflect PIPEDA's 10 privacy principles. The CMA's privacy code strives to give consumers control of their personal information and to make the process of gathering and using customer information by marketers more transparent.

The CMA code is recognized as the best practices document for Canada's marketing community and is viewed by many governments and regulatory bodies as the benchmark for ethical marketing and effective industry self-regulation. For example, the CMA was one of the 10 members of the federal anti-spam task force, which used the code as an important guide to the best practices of ethical marketers. Adherence to the CMA code of ethics is mandatory for all CMA members as a condition of their membership in the association.

The CMA code is also a continually evolving document. The association regularly monitors the marketplace to ensure that its code keeps pace with new marketing practices and technologies. Over the years, it has struck several task forces to consider emerging issues.

● (1545)

As the privacy environment has evolved, so too have the self-regulatory requirements and guidelines governing the activities of CMA members.

For example, in 1999 and 2002, the CMA concluded examinations of the sensitive issues surrounding marketing to children and teenagers, and revised the code to provide marketers with clear guidance on appropriate business practices for marketing to these distinct demographics. Among other requirements, collecting or requesting personal information from children under 13 requires the express consent of a parent or guardian, and all marketing communications must be age appropriate and presented in simple language that is easily understood by children.

A few years later, in response to the introductions of new technologies, marketing techniques, and regulations, CMA task forces critically reviewed Internet marketing activities, issued new self-regulatory guidelines for the industry at large, and amended the code of ethics with new mandatory provisions for its members, including requirements to identify the purposes for the collection and use of email addresses, to engage in email marketing with unknown parties only with consent, and to provide a clear and easy to use unsubscribe link.

In 2010, the CMA revised its code of ethics to provide members with guidance on marketing best practices for online, interest-based advertising, also known as behavioural advertising, which is perhaps most relevant to the committee's study. The new requirements cover transparency, consumer choice, and marketing to children when using this marketing technique and stem from discussions among the CMA ethics and privacy committee and with other Canadian associations.

More specifically, on the subject of transparency, the guidelines require that marketers using online, interest-based advertising should ensure that they, and the ad networks and website publishers that display interest-based ads on their behalf, provide clear explanatory information about how browsing information is collected and used, and provide an effective means to draw consumers' attention to that information. With respect to consumer choice, the code requires marketers to take the appropriate steps to ensure that the ad networks and website publishers used to display interest-based ads on their behalf offer consumers a clear, easy to see, easy to understand, and easy to execute means to opt out from having their online activities tracked over time to support the delivery of tailored marketing offers.

Finally, on the topic of marketing to children, consistent with the association's existing guidelines, the interest-based advertising guidelines prohibit marketers from engaging in online, interest-based advertising directed at children under age 13, except where express opt-in consent has been obtained separately from parents or guardians.

In conclusion, the Internet in general and social media in particular have opened up tremendous opportunities for individuals, society, and business, fundamentally shifting how we connect with each other, democratizing media, and presenting new and innovative ways for businesses to interact with their existing customers and grow their customer base. At the same time, consumers are demanding more tailored offers, convenience, and better service, requiring business to become more sophisticated to be able to anticipate and meet these needs.

To be sure, as we move toward the great promise of the rapidly developing information-based economy, some privacy challenges have arisen along the way for marketers and consumers alike. However, as the features and capabilities of social media emerge, and as consumer awareness and expectations evolve, these challenges are being addressed and overcome. This is because, regardless of any legal requirements or sanctions, legitimate businesses have every incentive to anticipate consumer privacy needs and resolve any concerns.

Canadian marketers have long recognized that consumer confidence is of paramount importance, and that privacy protections and transparent information practices are the foundation of their continued success. Simply put, marketers know that respect for personal information is good for business, whether online or in the bricks-and-mortar world.

I thank the committee for its attention and would be pleased to answer any questions honourable members may have.

● (1550)

[*Translation*]

The Chair: Thank you for making your presentation.

Without further ado, we will yield the floor to Mr. Zushman, from Merchant Law Group. He will make his presentation from Winnipeg.

Mr. Zushman, go ahead.

[*English*]

Mr. Jason Zushman (Attorney, Merchant Law Group): Very good. Thank you, Mr. Chair.

My name is Jason Zushman and I am a lawyer practising law in Winnipeg, Manitoba.

Good afternoon, Mr. Chair and honourable members. I am humbled to be asked to speak with you this afternoon with regard to privacy and social media. I look forward to our discussion which will touch upon these important issues that affect the lives of so many Canadians.

It's become cool to share information about ourselves, and it's become cool to share a lot of information. On a daily basis Canadians share an overwhelming amount about their daily lives. By way of example, there are over 18.5 million Canadians on Facebook, around 55% of our population. That is a shocking number in comparison to what Facebook was even just a few years ago. Because of this broad reach, adequate legal protections are necessary for the benefit of all Canadians.

The technological world and the Internet have changed many aspects of our societal interaction. The sharing of information is immediate. There are many benefits from our ability to share information in such a broad fashion, but there are also dangers that are found in this rapid evolution where technological advent can outpace the ability of Parliament and the applicable law to keep up.

As we analyze the issues related to online privacy, we should note that threats to the privacy of information shared by Canadians are found not solely on what are commonly thought of as conventional social networking sites. Threats to personal information can be found in quasi-networking sites such as online gaming communities. Many of these sites are pay-for services that contain sensitive information. If these sites suffer a successful hack or breach, they can reveal critically confidential user information such as home addresses and credit card numbers to rogue individuals.

As the online presence of many users can be correlated with their names, phone numbers, emails, and passwords that are found on their profiles in the conventional social networking sphere, identity theft can become that much easier. Many users have identical passwords or other means of access that are duplicated throughout the existence of their online presence. A breach of one of these services can lead to a breach of all services that are used by these Canadians.

Specifically, I would like to comment with a view to privacy and social media aspects. I wish to share the following observations.

First, the provision of informed consent by the user is a necessity. That means when a user gives their consent to utilize the service, they must be asked to give consent throughout the entire process and for any subsequent evolution of that service or its terms of use. Users shouldn't be asked merely to provide their initial grant of consent to terms that could then be unilaterally modified by the service provider.

At times when a user submits information to a social networking service, they do so with the intent of limiting the release of their submitted information to a trusted circle. It can cause great harm and unexpected consequences when the information that those users share is subsequently treated in a different fashion than what that user had originally intended. When the terms of use are changed or subsequently modified by the service provider, that modification must require the fresh consent of the user prior to the change and the implementation of the new terms.

Many times the user is placed in a position where the modification of the terms is simply displayed in a pop-up window which may be given only a cursory inspection by the user and can be over-shadowed by the user's desire to return to their social media experience. Users may not always be given a means by which they can continue to use their service ostensibly without their agreement to the newly modified terms.

All changes should be clearly communicated to the user, and users should be made aware of any substantial impact to their rights. It is paramount that users always be made aware of how the information they provide is used and retained and how steps can be taken that allow for its removal from the social media site. Further, users should be told exactly how their online habits are being tracked and how that collection of information that determines their psycho-graphic, or we have seen recently with facial recognition software, their biometric makeup is harvested for purposes such as ad placement or other such uses.

Users should also be told to what degree this information is shared not only within the organization but also with the public and also how it is shared with any third parties for which certain uses of that information are not necessarily foreseen by the initial contract that the user enters into with the social media provider.

● (1555)

Second, I think we require more robust privacy laws. If breaches to personal information do occur, there should be laws that effect meaningful and substantive remedies. Powerful consequence-oriented law will deter an organization from engaging in an unauthorized practice in the first place. Further, such laws provide incentive for organizations to take preventive measures prior to the occurrence of a privacy breach, or any modification of terms that result in the unauthorized use or release of user information.

Any use, unilateral change, or subsequent modification of the terms that grant access to that user information, for which consent has not been provided, should have meaningful consequences. Misuse of information that is provided in good faith by users should not simply be calculated as a cost of doing business. It may be of benefit to consider laws that provide for quantification of damages that are in direct relation to the profit, or to multiples of profit, that the misuse of this user information has provided to the companies that are in play. To my mind, robust parliamentary solutions that enhance and shore up our privacy laws will go a long way to ensuring that the privacy of Canadians is truly acknowledged and respected.

There is a third point I'd like to discuss. I noticed that Mr. Péladeau spoke to rules regarding a contest, I believe, that was offered by Sleemans, and how it exported some of the potential legal protections that were available to, perhaps, law that was not applicable within the Canadian sphere.

Finally, I'd like to speak to the use of form selection clauses. As I previously discussed, most of the terms of service to which the consumer agrees to be bound are boilerplate or standard form contracts, and those contracts are crafted in the language of the issuer or the social media site. There is no real bargaining power on the part of the consumer to change or to modify the terms of these agreements.

As we engage in a lively debate about the potential change of law and the grant of powers to those who would be able to enforce consequences against those in the social media sphere that may not respect the privacy rights of Canadians, I would like to say to the committee that contained within many of the contracts of service offered by these social media sites are what we refer to in law as choice of law or form selection clauses. These clauses aren't necessarily easily understood by the consumer, but they are engineered to have a very practical and beneficial consequence by the draftsperson.

It is all fine and good to have a body of tort law and statutory codifications that place privacy in high regard and that protect Canadians, but this is all in vain when a dispute arises and Canadians are potentially told that the agreements they have entered into don't allow for the application of that same Canadian law. Instead, Canadians are told that their social media use or breaches of privacy that arise pursuant to that use, is instead governed by the laws of California or the laws of New York.

Pursuant to a form selection clause, our domestic law may be displaced and any available remedies are to be made subsequent to foreign law, a law that doesn't necessarily reflect the values and protections that we hold dear as Canadians. It is essential when organizations target Canadians and use their personal information with a view to profit, that meaningful consequences can be brought to bear if that same information is abused. It is essential that Canadians are protected by the laws that are enacted by Parliament so they can be assured that the societal legal norms that we have established are respected and enforced.

Many social media companies explicitly cater toward Canadians for their profit. They accept and they run local advertisements. They have head offices that are set up in Canada. They offer promotions and services that are tailored to our national experience. When these companies make the choice to conduct their business in Canada by catering to our local trades, they should be willing to similarly acknowledge and conform to the laws and consequence that exist within our jurisdiction.

I would like to recap the three primary points I'd like to stress from my observation for the committee's consideration.

The first would be informed consent for the user. That informed consent must be required not only for a user's initial grant of use, as related to their personal information, but also for the subsequent modification of terms that will affect the user's experience or the social media company's use of that personal information.

Second, I believe that privacy laws should become more robust. Effective consequences should be brought to bear in relation to damages in tort, common law, or other breaches of statute. Consequences should be strictly enforced to effect deterrence and to protect the privacy rights of all Canadians.

● (1600)

The third thing I'd like to stress is the jurisdictional aspect. An essential component of any parliamentary response to privacy law should displace the need for the legal test known as real and substantial connection, to establish a jurisdiction simpliciter, and to have jurisdiction over the subject matter to which Canadian law can be applied.

It should be made clear and unambiguous that companies choosing to do business in Canada will be bound by Canadian law. I believe this should be explicitly codified.

Thank you very much for the opportunity to appear before you today. I look forward to answering any questions you might have this afternoon.

[*Translation*]

The Chair: Thank you, Mr. Zushman. I want to thank all three witnesses.

We will now begin the question and comment period. I yield the floor to Ms. Borg. She has seven minutes.

Ms. Charmaine Borg (Terrebonne—Blainville, NDP): Thank you, Mr. Chair. I want to thank the witnesses for joining us today.

This issue is extremely important to us, and I am sure it is also important to you since you have come to see us and you do a lot of work in that area.

The committee members have just come back from Washington. We had lengthy discussions on this topic with our American neighbours, and we talked about what they were doing. We discussed this topic with them thoroughly. They said that, as parliamentarians, we should not regulate that growing technological sector too much, since we don't want to discourage innovation.

Mr. Péladeau, what are your thoughts on that? Are we necessarily sacrificing innovation by imposing the regulations? If not, is there a balance we could strike?

Mr. Pierrôt Péladeau: Here is the short answer. The issue is being raised in the United States. In 1986, I participated in a study the Government of Quebec commissioned to look at all the laws in the world. One particularity of the American laws, when compared with all the other laws in the world, is that the Americans focused too much on details in their regulations. They were tinkering too much, and that froze innovation. That's why I said earlier that personal information protection legislation should apply to the development phases and not to procedures. That was actually one of the recommendations set out in the report called *L'identité piratée*, where that approach was recommended regarding Quebec's personal information protection legislation. I understand that legislative approach in the U.S. context.

However, Canadian and European laws are more broad. They don't necessarily impose any procedures. They set management objectives that apply more broadly to the production, storage and communication of information. Companies are left with the responsibility to enforce those laws. That approach is more robust with regard to technological evolution, and it enables companies and organizations to enforce the laws.

Since then, I have noted that those are basically sound governance rules, as I was saying earlier. If sound governance rules are applied, companies will benefit. I will give you three quick examples.

In a large communication services company, they realized that the section covering Montreal Island produced 80,000 memos a month. It took one to three minutes to write those memos, which were totally useless and overburdened people who provided customer service. When I did the work in 1995, I realized that small companies, such as day-care centres, consisted of very small units: a secretary and a business manager. At the time, we succeeded in reducing the quantity of useless information managed to the equivalent of three months per person, to say nothing of the impact that had on the service.

In short, there should be as much involvement as possible in logical information phases—the major phases of the information life cycle—and not procedure phases, so as not to complicate everyone's life.

As I was saying, we must also realize that, when it comes to personal information protection, we should stick to sound governance and transparency rules. Issues such as child consent can be resolved from the outside. That matter does not apply only to the use of personal information, but also to all interactions with children. That may be held as a separate and universal principle.

To summarize, we should not deal with this in a sector-based way, like in the United States, or in such a detailed way, but rather as universally as possible, based on governance phases and principles.

● (1605)

Ms. Charmaine Borg: My next question is again for you, Mr. Péladeau.

Do you think that a lack of trust and transparency may stand in the way of developing the full potential of social networks as a democratic tool?

Mr. Pierrôt Péladeau: Yes, that's a fact. We don't have enough feedback to verify that and be able to confirm it. However, there are very clear signs. The Facebook case speaks for itself. Facebook made certain changes that were disliked by its members. They reacted strongly. That made us realize that, basically, relationships are being managed. The trust relationship issue is a key element.

That being said, trust aside, we should understand that some of those applications develop in a local monopoly. It's a temporary condition, but we are talking about a monopoly.

Let's look at the Facebook case again. In some schools and classes, if you are not on Facebook, you are not part of the gang. Market mechanisms exist. We see them operating on a macroeconomic level. However, when we consider them from the individual's microsociological situation, we see that people don't necessarily have the option to be part of one group or another.

I have a very simple example for you. I have been a grandfather for 18 months. I had to join Facebook to see photographs of my grandson. My daughter is on Facebook and has about a hundred contacts. So although I would have preferred for her to use Google+, Flickr or another site, she told me that Facebook was the place to be, and thus left me no choice. So trust has an influence on a community level. However, it cannot necessarily have an influence on an individual level because market mechanisms are unavailable.

That has a consequence. If market mechanisms are not necessarily available, other mechanisms need to be used. If the walking is not working, we need to use talking. That's why I was saying that processes must be as transparent as possible. People must be allowed to make their own decisions and change the parameters themselves in full knowledge of the facts.

That social medium imposes a set of rules on us. It's an exercise of social power I have to participate in. As I was saying, the market mechanism does not necessarily work on an individual level. However, on a community level, social media are a place for discussion where communities of members can enter into a relationship—into what I earlier referred to as a democratic dialogue—with the developers and operators of those systems.

The legislator must ensure that this happens transparently. Afterwards, we must rely on social relationships and communities to decide in what direction things should move. That's how we can call for a boycott or service change, as people are doing at universities, where various social media are being used to discuss matters with students. They can decide together to go elsewhere if that is not working.

That along with privacy protection laws helps achieve transparency and hold a dialogue among individuals or a community, on the one hand, and the operators of those systems, on the other hand.

● (1610)

The Chair: Thank you. I have to cut you off.

I want to remind everyone that the seven-minute period includes both questions and answers.

It is now over to Mr. Calkins.

[*English*]

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

I have a couple of questions, but first I want to preface with my mindset that there are two schools of thought on this. One approach would be to pursue a more stringent regulatory approach that would be quite cumbersome, quite slow moving in trying to keep up with the pace of the ever-evolving technology and the innovative uses of that technology in today's social media environment. The other approach would be to simplify and codify a set of ethics standards or rules governing what should be proper use and then provide a hammer when somebody steps out of line.

Whether it be through civil litigation or other types of, shall we say, social licence challenges, we've already seen responses from those companies where their practices have been exposed quite publicly.

I'm going to ask Mr. Elder and Mr. Zushman which approach they would prefer and which one they think might be more beneficial. Would it be giving more power to a privacy commissioner to apply the basic rules and guidelines, and when those things get out of hand to maybe apply a disciplinary approach, or should we get into the business of trying to create a huge regulatory approach in trying to govern some of these issues?

Mr. David Elder: Is it an option to do neither of those?

Mr. Blaine Calkins: I suppose it's an option to do both, and it's an option to do neither. I would like to get your opinion.

Mr. David Elder: I would argue that we've come somewhat close, I think, to option number two in terms of simplifying and codifying an approach. This is exactly what PIPEDA does, recognizing that technology is evolving very rapidly and the legislative process will always be behind. PIPEDA takes the approach that sets out basic principles that all organizations must follow. That allows for a great deal of flexibility to users and ultimately to a privacy commissioner in determining what is required, what level of disclosure, what type of consent, and what sort of uses are within the reasonable expectation of consumers, etc.

I think we're very close to having the right approach.

With respect to more powers to privacy commissioners to enforce, I would say that for many businesses, certainly the larger and more reputable businesses, fines and those kinds of enforcement powers are almost beside the point. The real stick, and where the rubber really hits the road for such companies, is the type of publicity you described.

When there is a major privacy breach and the company's name is all over the headlines about being hacked or about doing something inappropriate with data, that really does a lot to damage the company's brand. It makes people question their trust in the company. It makes people think that maybe they should be using alternate providers. Regardless of what the laws might be, that is what most businesses are really focused on.

One of the problems with having more enforcement powers is that it changes the essential nature of the relationship between privacy commissioners and business. Right now we generally have a fairly cooperative, sort of ombudsman-type model. I think it works fairly well. That is more conducive to organizations proactively sharing information with privacy commissioners.

If we move to a regime where there are more sanctions to be applied, it becomes much more like litigation, and I don't think that's the environment we want for privacy in Canada.

Mr. Blaine Calkins: Thank you.

Mr. Zushman, do you have any comments on this?

● (1615)

Mr. Jason Zushman: Yes, I do.

First of all, the privacy commissioner performs an essential role. There is the question as to whether you would give more powers to the privacy commissioner or you would lead to a hybrid sort of judicial model where you're describing different statutes and codifications that would give more power to enforce litigation.

Part of the theory seems to be that when a company receives bad publicity—shall we say, the changes that were enacted by Facebook in 2009—consumers at that point proceed to vote with their feet and the company doesn't want to be seen in that particular light. But as we've heard from Mr. Péladeau, it becomes a social norm to be part of Facebook. It becomes a social norm to be part of these other social media sites, so people still return even though they realize there have been affronts to their rights, which can occur.

Perhaps you could also look at developing a hybrid model by which you could have the cooperation of businesses and different companies within the social media sphere with whom you could work to jointly develop those same laws and regulations, which could then be utilized for the protection of all Canadians and their privacy.

Mr. Blaine Calkins: My next line of questioning comes from just a little bit of personal experience I've had. Believe it or not, I had a life before politics. I was a database administrator, and I understand that corporate data is a company's greatest asset, outside of its human resources. Of course what we're talking about here is what we do with data that's collected wittingly or unwittingly, knowingly or unknowingly, and how it's utilized after the fact, whether it's identifying an individual personally or whether it's data that's simply collected and assembled into information to provide marketing research or whatever is prevalent today.

The informed consent question is one I think we need to flesh out. We've heard many witnesses here talk about the devil being in the default settings that apply. We've heard horror stories, with all due respect to the lawyers in the room, about 15 pages of legal jargon. Of course users have a choice to either accept or not accept all of it in its entirety, perhaps without even knowing exactly what it is they're agreeing to.

Would I get consensus from the three of you that there needs to be a more simple process by which end users can be engaged in this and have confidence in knowing what it is they're agreeing to when they choose to use a free app they've downloaded, when they choose to sign up on a Facebook site or anything else of that particular nature, which may or may not track their personal use and information while online?

[*Translation*]

The Chair: Time is up, but I will give each of you 30 seconds or so if you would like to answer the question.

[*English*]

Mr. David Elder: I'll jump in.

Certainly, one of the most difficult things is getting this balance exactly right. As a former chief privacy officer, I can tell you that it's extremely frustrating. On the one hand, you'll have people saying that it's too short, that you didn't disclose this and that. On the other hand, if you put everything in your privacy policy, you get accused of having a document that's longer than the Declaration of Independence.

I think we're starting to move toward models, and the web itself provides a great model for this. We're seeing layered policies where all of it is there, but it's presented through a series of hyperlinks that allow users to get very quickly to the aspects that are of particular concern to them, and therefore they can inform themselves and make an educated choice about how they want to proceed.

[*Translation*]

Mr. Pierrôt Péladeau: I agree. It's another process. As I said earlier, it's not done in an upfront way, where users are given a form to fill out once, and that's it. The process has to be ongoing. An interactive solution would allow users not just to access hyperlinks, but also to see what's going on. Text isn't the only option. A pop-up window could appear to tell people that if they do something in particular, their information will be sent to person X. The message could also tell people what the information will be used for. That would be a visual solution. We have to find Internet-based methods, because the Web gives us that kind of flexibility.

I think my 30 seconds are already up.

[*English*]

Mr. Jason Zushman: Just to chime in, yes, you would obviously receive my consent to the terms and conditions that a user would agree are more straightforward and simple.

I guess it becomes difficult for users to provide consent potentially to unseen or unforeseen uses of data, for example, facial recognition. Let's say you upload a photo. A future development in that technology related to the use of that photo could be something that the user wouldn't necessarily consent to. To my mind that would be found in the ability to recall and remove the information that a user has provided from the social network.

But, yes, simplicity would be advantageous for sure.

● (1620)

[*Translation*]

The Chair: Thank you.

Mr. Andrews, you have seven minutes.

[*English*]

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

We'll come back to simplifying the consent form, Jason, in a minute.

My first question is for you, David.

You mentioned that the CMA has a code that is self-regulatory, and that your members adhere to it. Just to put it in perspective, could you give us some idea of what your membership is in Canada? How many marketers are members?

Mr. David Elder: It shifts all the time, but we have somewhere over 800 members. I'm not sure how that comes out as an exact percentage of marketers and advertisers in Canada. I could certainly undertake to try to get you that figure, but my belief is it certainly represents a substantial majority of major Canadian marketers and advertisers.

Mr. Scott Andrews: Okay. In our role we try to catch all, and it's hard to do that.

We were told by some of these Internet companies that the marketers do not actually see the personal information; rather, they are marketing people of general demographics or general consent. They don't actually see that Scott Andrews is a male between the ages of 35 and 40, but that you'd market to that. Is that true? How much data do these marketing companies actually get?

Mr. David Elder: In what context are we talking about? Are we talking about in social media?

Mr. Scott Andrews: Yes, in social media.

Mr. David Elder: Well, it depends on whether or not you are a social media platform or not. We've been talking about Facebook a lot. Obviously, Facebook has quite a bit of data and has all of your profile information. They have that information.

I certainly don't speak for Facebook, but my understanding is that for the most part, they keep that data to themselves. It's their greatest asset, it's not something—

Mr. Scott Andrews: What do they provide to the marketers?

Mr. David Elder: What they provide to marketers is access to the platforms. They'll say to the marketers, “We won't give this to you, but you tell us what kind of people you want to hit, for example, members of the ethics committee, and we'll do our best to direct your ads to those people.”

A similar thing is, if you are the marketer, obviously, you won't have that information. You will indicate your target group and say that you're looking for certain characteristics. Then a social media platform will do its best to display it to those people. Certainly, the advertisers don't have access to that.

Mr. Scott Andrews: Is that common throughout, or are we only talking Google and Facebook throughout all these applications?

Mr. David Elder: It's hard to generalize, but for the most part, that is true. Again, that's a big piece of what the business is for those companies. Once they hand over that detailed information to another party, putting aside the privacy issues involved in that, they've given away the store, in a way. That's their main selling point.

Mr. Scott Andrews: Okay.

Jason, I'll turn to you now.

Your company was successful in a class action lawsuit against Facebook a few years ago. Was this a worthwhile exercise to go through? Did you see that Facebook actually changed their practices? Is this a way of keeping them on their toes?

As a second part to that question, we were also told that these companies set the bar wherever they're challenged. If they're rapped on the knuckles for one thing, they set the bar there. If something else happens, the bar keeps changing.

Is that true, and does that apply across all countries that these companies are in? If they get rapped on the knuckles by a Canadian company or Canadian users, is that the same bar for the rest of their users in other countries?

Mr. Jason Zushman: Thank you for the question, Mr. Andrews.

I can't speak specifically to their activities in other countries.

The Facebook class action was a worthwhile exercise, during which we had developed changes in response to the different treatment that Facebook had of user data. I have noticed a tendency that Facebook, to my mind, seems to introduce a set of changed conditions and terms; they respond to the public response to the changed conditions and terms and roll it back, and then at a future point, those terms may be reintroduced.

They set the bar at a level. There's public response and a backlash. Then those terms and uses sometimes end up working their way into the Facebook system regardless.

I do think that greater legislation is required in order to effect meaningful consequences for these companies.

● (1625)

Mr. Scott Andrews: That leads me to another question. I think you said in your third point that you thought about codifying that. Can you tell us specifically how we'd go about doing that? Across all these different social media, how do we codify this and make it simple?

Mr. Jason Zushman: That's a subject for a very lengthy debate on which we could canvass. I had at first thought about studies just like this one. I also had thought about reaching out to industry as one way to do it, and to see different ways that they could allow for people's privacy.

I guess what I don't want to see is a wholesale exposition of data that's offered by Canadians to these companies in good faith and that's subsequently used for unintended purposes. I think that's something that should be looked at by Parliament to craft an adequate response.

Mr. Scott Andrews: Moving on to the issue of simplified consent forms, often we see multiple pages. How do we get these consent forms down to something that is reasonable, and what is reasonable?

Mr. Jason Zushman: The choice of jurisdiction clause is something that should be boiled down to simply saying that [*Technical difficulty—Editor*] afforded to you in Canada may not exist should you choose to enter into the service.

Facebook at one point was criticized, as our earlier witness stated, for having terms of service that were as long, if not longer, than the Declaration of Independence.

I think that key primary points should be addressed. If a pop-up occurs in a window, the key primary points as to how that will affect the user in very short language should at least inform the first part of that pop-up. A lot of times what happens is that the entirety of the terms and service changes are reproduced within that pop-up window, and the "accept" button is featured when the pop-up window occurs. You can click "accept" without necessarily scrolling down through the multitude of terms and changes to the conditions that occur. I know that there was technology employed at one point that required the user at least to scroll down to say that they had looked through the terms—they'd had a cursory glance—before they could click accept.

I do think that simplification exists.

Mr. Scott Andrews: How do we condense that into two paragraphs? Can we or are we dreaming?

[*Translation*]

The Chair: Mr. Zushman, I'll give you 30 seconds to respond.

[*English*]

Mr. Jason Zushman: That is a complex issue. I think that the primary terms that affect the change should be reduced.

[*Translation*]

The Chair: Mr. Carmichael, you may go ahead.

You have seven minutes.

[*English*]

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

As we're listening to the questioning, it's clear the reason we're here today is we all agree that social media companies—I don't know that I'd necessarily include all of the marketing companies because I'm not quite sure where the definition, where the boundary is between them—push the boundaries of the rules to their outer limits and then apologize when they've transgressed or they've been called to account for what they're doing.

One of my colleagues talked about our trip to Washington last week. We heard lots of feedback and testimony with regard to the new U.S. framework, which is evidently more broadly based than the new European guidelines, but more stringent than it has been. The regulations are coming out this week, if I'm not mistaken. We're seeing in different countries and parts of the world different responses to what is clearly a serious problem.

My biggest issue is data collection. Where does it go and do consumers, do Internet users, have any control? Our Privacy Commissioner has made the statement that it's freely given. I think she was right that we who use Facebook or any other social media freely give all kinds of information without any idea of where it's going or how it's going to be used, whether it's used for marketing purposes or whatever else. Then in the event of a breach of security, you've got a bigger problem. You have all kinds of threats that can come at the various Internet users, the individuals.

Can Internet users have any control over their information or any greater access to know what they've actually submitted or what's out there on them? I wonder if there's any way an Internet user can be in any form of control over the data that's shared on the Internet.

Mr. Elder, let's start with you.

● (1630)

Mr. David Elder: I think that users have a number of means of control on the Internet. Some of those controls are featured in browser preferences. For example, you can set up browsers for various safe zones to reject or accept certain cookies and other types of information. When users are using the Internet, when they're using a social media application, they certainly have control over what they post, how they post it, whether they put in their full birth date for example and put it on their homepage, and whether they make that viewable by anybody who is surfing the Internet.

Moving forward, and I don't know whether you heard about this when you were in Washington, there are initiatives looking at things like interest-based advertising in the U.S.A. which we're working on bringing to Canada and Canadianizing. This is the Digital Advertising Alliance, DAA, initiative. Sometimes when you're surfing you may see a little triangle with an "i" in it on an ad. You can click on that and it will give you information about why you're seeing that ad, why it's being displayed to you.

It will also give you options to go to a centralized page where you can choose whether or not you want it to be placed in cookies on your machine to give you that kind of targeted advertising. It gives you quite a bit of choice as to whether you don't want to receive any or you don't want certain companies sending you targeted ads and collecting information. There's quite a bit of leeway for user choice.

Mr. Jason Zushman: Coming back to the simplicity of the picture example, I would have concerns about unforeseen uses of data that can potentially occur. The general rule is that once you've shared information on the Internet, it's difficult to guarantee that you'll have any right of retrieving that information; it could very well be out there for good. For example, if a user shares information through Facebook and Facebook has a third party application that's engineered and the user subsequently enters into an agreement to allow that app to use the data that the user has provided, what guarantee does the user have that the third party application developer won't necessarily go rogue?

There's a different transit of information. There's a transit from the user of that picture to Facebook, a use by the third party application developer of that photo. What does the third party application developer ultimately do with that photo? What uses could that have that are outside of Facebook's ability to recall and outside of the user's ability to retrieve? That would be a concern that I would have.

Mr. John Carmichael: Thank you.

Mr. Péladeau, did you want to weigh in on this one?

Mr. Pierrôt Péladeau: Yes.

Some models are being developed. Unfortunately I cannot remember its name but one developer is trying to develop a kind of control panel on the flow of information so the user, not social media, would control and own information. Technically all this is using Turing machines. They are machines that could apply any kind of algorithm you could imagine. Technically it is possible to conceive alternative models.

The issue is how we get there and that's clearly from the existing framework. Right now it's wide open, and we don't want to infringe on innovation.

Theoretically it is possible. People are working on it, but I know of no one who knows the road to get there to achieve this.

● (1635)

Mr. John Carmichael: That's it?

[*Translation*]

The Chair: Mr. Carmichael, you're out of time.

I will hand the floor over to Mr. Angus for five minutes.

[*English*]

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

Thank you, gentlemen. This has been a fascinating discussion.

I think we certainly agree, Mr. Elder, we are just on the cusp of the change in the market, in democratization, in innovation from new media. I think we are all committed as a committee to try to find a way to ensure that innovation continues. The question is what happens when the breaches occur, because we're not talking about niceties in these breaches. We're talking issues of identify theft, victimization, and breaches of law and international law. There are serious issues. However, if we step in where we as legislators don't know where we're going, we could seriously impact the development of all manner of ideas and marketing.

I'm very pleased that your marketing organization has a code of ethics. What's interesting is the democratization of business as well. It seems now that the big players are having to adapt and be like small players, because new media favours small start-ups. It favours people who would never have been able to put their ads in a newspaper before. They use Twitter, Facebook, Tumblr, anything else. Now the big guys are having to play with small players, and I think that's fascinating.

Mr. Elder, you say status quo, but then what about the outliers? Should there not be, through the Privacy Commissioner, the tools to ensure that there's predictability in the market so that your guys play by the rules, but for the ones that don't there's a way we can bring them to heel?

Mr. David Elder: There's a way now. We already have a situation where things can be investigated by the Privacy Commissioner. She can make a report of findings. She can decide, or the complainant can decide to bring that matter before the Federal Court. The Federal Court can issue any order, including injunctive relief or awards of damages.

Mr. Charlie Angus: We've heard from the Privacy Commissioner and from many others. PIPEDA has played a role. The world has looked to PIPEDA. They're saying the lack of administrative monetary penalties is now starting to catch up to us because everything else is moving so fast.

Would you support her ability to bring in administrative monetary penalties? Your organization is playing by the rules but there are people out there who aren't.

Mr. David Elder: Again, as I said earlier, I think when you give an ombudsman, an investigative body, the power to also order fines, that fundamentally changes the balance and you have someone become investigator, judge, and jury. That would be to the detriment of what for the most part is an open and fruitful dialogue on privacy issues between the Privacy Commissioner's office and the business community. Routinely now when companies are introducing a new service or feature or technology they call up the Privacy Commissioner's office and give her a briefing. I cannot guarantee, but I would predict that in a different model we'd see an awful lot less of that.

Mr. Charlie Angus: That's interesting. I wonder if we're dealing with a false dichotomy between innovation and rules because we need predictability. Right now what we're dealing with is like the wild west out there. It's leading to a lot of great things, but the damages or the threat is certainly there. The question is how do we achieve that?

Mr. Zushman, you suggest Parliament. Would you not agree that the Privacy Commissioner is better equipped to stay on top of this than having us sit around in a room here, hearing about the facts a year or two later, trying to come up with legislation, trying to cobble the pieces together? If the Privacy Commissioner were given the tools that she or he needed at the time, we would be able to stay in the game without unnecessarily interfering with its development. Would you suggest that the Privacy Commissioner should have administrative monetary penalties?

● (1640)

Mr. Jason Zushman: Yes, Mr. Angus, I appreciate your classification of dichotomy. I do think that the Privacy Commissioner deals with these issues every day. I think the deference that could be given to the Privacy Commissioner's ability to solve these matters would be inside her area of expertise. I would be in support of monetary penalties by way of her discretion, after a full and final resolution and canvass of the issues that she would deem appropriate to be investigated had concluded. I would agree with you.

Mr. Charlie Angus: Quickly, Mr. Péladeau, and following on the same line, when we don't have clear rules and penalties and we do see the rise of class actions—we have seen a number of class actions recently—those can impede development as well. Would you see that predictability would be enhanced in terms of, as you say, picking the big principles, but then giving the Privacy Commissioner the power to enforce that? Would that put us on a better legislative frame than having to rely either on class action or on voluntary compliance?

[*Translation*]

The Chair: You are out of time, but I will give Mr. Péladeau a chance to respond.

Mr. Pierrôt Péladeau: What it comes down to is establishing the rules across the board, especially since new players are always entering the field, including young go-getters. Predictability is key because a lot of start-ups in the market right now don't yet have business models in place. They don't know how they will go about monetizing their relationships with customers and so forth.

If there were rules, businesses would know which doors were closed, which ones were open and what society expects in that area. Innovation isn't a natural phenomenon; it's the product of the marketplace and social rules. In that sense, a significant step towards innovation would be to say you have to put the consumer and user-friendliness above other considerations.

The Chair: Thank you.

I will now turn it over to Mr. Dreeshen for five minutes.

[*English*]

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

Thanks to all our guests.

I, too, was in Washington. We spoke to a lot of industry leaders and regulators. We were talking about disincentives as far as innovation was concerned. A few of my colleagues have described that as well. I think it's an important issue.

Mr. Elder, I'm not sure whether you've had an opportunity to go through that and see what the feelings of the members you represent are in regard to that particular area. To go back to some of the other comments that were presented, when you look at the ability to have ads that are specific to an individual, it's like going into a car dealership where everybody is on commission. This is a case where everybody is going to want to get at you, so I don't really see the difference. If you've indicated that you are interested in vehicles, then there is the possibility that they can get the information to you. That's why we get the Internet for the price that we do, because there is advertising.

Perhaps you could talk about that from the industry point of view as to the significance of their ability to get information to the user, and the significance it has for the general concept of the Internet and its usability for all individuals.

Mr. David Elder: Are you talking about it in the context of a targeted advertising position?

Mr. Earl Dreeshen: Yes.

Mr. David Elder: Yes, I think there are great benefits to interest-based advertising, as you suggest. It has certainly been explicitly acknowledged by the Privacy Commissioner.

Much of the Internet is free to use, particularly the social media applications. There are some “freemium” options on some of the sites, where you can pay a little extra money for extra features, but most of the major ones that people use for hours every day cost them nothing. They are advertiser supported.

The advertising you might send off to somebody in the vain hope they might connect and that it might resonate with them is worth less than an ad that you can try to direct more precisely to someone who might actually be interested in that product or service. The availability of those types of ads does a great deal to help lift these applications on which we rely.

For users, I can tell you that we're going to see ads on these things whether we like it or not. They're advertiser supported. It's a bit like television. We might think to ourselves that if someone were to give us the choice, we would rather not see any ads when we're watching a TV show. Well, if you don't see the ads, you're not going to see the TV show, because that's what pays for it. If they're going to see ads, I think a lot of users would rather see ones that actually do have some relevance to their wants, needs, and values.

● (1645)

Mr. Earl Dreeshen: Mr. Zushman, do you have a comment to make in that regard?

Mr. Jason Zushman: Personally, I guess I would take issue with the description of these services as being free. I think that the archiving and monitoring of information that's provided by users is what provides the monetary benefit to the companies. I would shudder to think of what the value of the database collected by a lot of these social media companies is, because that's where the real value is.

I also think it's a little different if consent has been given and a consumer explicitly requests, let's say, advertising for a new Ford pickup. It's an entirely different matter, I think, when a user types something into their update panel that talks about memories they had when they were young that concern good memories of riding around in a Ford pickup truck, and then all of a sudden advertising for the Ford pickup truck is tailored toward that user response. I think there's a distinction that should be drawn there.

The monitoring is what provides the monetary value, so I don't necessarily agree that it's a free service, but I can see the position being put forward.

Mr. Earl Dreeshen: Monsieur Péladeau.

Mr. Pierrôt Péladeau: There are alternative models, and interest marketing is interesting for that, but it depends who controls the process.

Lately I had to buy a dining room table and I had to go through 32 stores before finding the right one. I would have liked to make a tender. Those models are being developed, where I could make that tender. I want a table that seats a certain number of people, and so on and so forth. I put it on a site without any information about me. I'm a buyer. When the right seller comes in, I will contact him. Don't call me; I'll call you.

Those models are possible, so that's why we must not impede those kinds of innovations. We must look forward in that direction. We could develop models that would be economically sound based on that. There are alternative models.

[*Translation*]

The Chair: Thank you. Unfortunately, your time is already up.

It is now Ms. Borg's turn for five minutes.

Ms. Charmaine Borg: Mr. Angus is going to start and then I will speak.

The Chair: Very well, you will each have two-and-a-half minutes.

[*English*]

Mr. Charlie Angus: Thank you.

I would like Mr. Zushman to talk about this jurisdiction clause, because I'm looking at a lack of consent by design. I get this form. If I want to use my Facebook site—and I'm not picking on Facebook—but if I want to use anything, I have to click on it and somewhere down in the 45,000 words it says that I'm governed by the laws of some other jurisdiction even though it's my data in my country. I would imagine most marketers want my data in my country.

How do we address that? I would be worried about going on a site and seeing, in 45,000 words, somewhere at the bottom, that all my financial transactions are governed by the laws of Somalia. You can certainly set it up in there, if you're not governed by the laws of the country that you're in. You could allow all manner of things.

Can we address that? Is that something we could zero in on and say this has to be fixed? It's my data. If it's in my jurisdiction I should be protected by the laws of my country, period.

Mr. Jason Zushman: Yes, Mr. Angus. Thank you for recognizing that point.

I tried to make that an integral part of the final portion of my presentation. The reason I did that is this. If we develop laws or we call on the Privacy Commissioner to enforce very real consequences, if the user has agreed and displaced the laws of the local forum for, as you would say, Somalia, what do you do when that comes before the courts? Or what happens when the Privacy Commissioner goes to actually enforce that judgment in a jurisdiction that doesn't have the reciprocal enforcements of what she is trying to declare as against that social media outlet?

I had put my mind to that briefly. I had thought it should be set up perhaps by way of legislation that could contain definitions as to what a social media company is. Also, social media companies that conduct business within the jurisdiction are clearly governed by the laws of Canada. You could have a voluntary method by which the large key players would voluntarily submit to be governed by that legislation if something like that is forthcoming.

I'm not sure if the appetite exists for that, but I guess there are different ways we could potentially analyze that issue.

● (1650)

Mr. Charlie Angus: If the big players adopted one of our recommendations about jurisdiction and laws of jurisdiction, it would set a standard that would be much easier to follow, but without our raising it as a parliamentary committee, Bob's your uncle, and things can carry on.

I'll pass it over to Madam Borg.

[*Translation*]

Ms. Charmaine Borg: Thank you.

Another thing we learned on our trip was that the FTC recommends establishing a list of parties sharing the information. It would target companies—not necessarily Facebook—that use information to sell products to certain people and for other reasons.

Mr. Elder, you said you represent about 800 members, but we don't know the scope of those companies. We don't know all of them. We're having trouble figuring out exactly who those people are.

My question is for all three witnesses. Is this a possible solution, given the need to improve transparency, so that people understand who the companies are and what they do with the personal information? Would that make things more accessible and transparent?

[*English*]

Mr. David Elder: I hope I understand your question. There is an access right under privacy law that says a user can have access to the information that an organization holds about him, and he has a right to know how it's being used and disclosed. You're saying there should be a list that names the organizations to whom that information—

Ms. Charmaine Borg: —and, most important, who the companies are, because it's something that very few people are aware of.

Mr. David Elder: The difficulty would be that those tend to be evolving relationships. For instance, if you buy a dining room set, to use Mr. Péladeau's example, you might consent at that point to release information to certain companies, but at any time it can be very difficult to track precisely to whom your data has been provided.

Ms. Charmaine Borg: Sorry, I'm just going to re-explain the model. What the FTC is suggesting is a website where you'd have, let's say, data broker companies X, Y, and Z designated as companies that use these lists and sell them or do whatever they want with them. They are in the business of data brokerage.

Mr. David Elder: Oh, I see.

Ms. Charmaine Borg: It would be published and accessible to the public so that they could know that these companies exist and what they do.

Mr. David Elder: I haven't really given that a lot of thought or spoken to the CMA about it, so I won't put this forward as the CMA's position, but I would say generally that companies are in favour of the concept of transparency and so to the extent that a company is collecting, using, and selling data to others, that sort of information should be available.

Mr. Pierrôt Péladeau: It looks a bit like the U.K. model where they have a registrar of some sort, and it's very bureaucratic. I'm not sure that this is the right way to go. But if there are standards of transparency and openness such that if you are in the market you must provide this or that information and make it available, that would make more sense. If the issue is to create a registrar, that's costly and you might not be covering everything. But if you have a clear obligation to be open and transparent, in the work we did in the "*L'identité piratée*" report in 1986, that was the model we preferred.

● (1655)

[*Translation*]

The Chair: Mr. Zushman, is there anything you would like to add briefly?

[*English*]

Mr. Jason Zushman: That was the point I was trying to stress before. If there is a primary entity by which the information is entered or shared and there are a bunch of sub-organizations taking care of that data—I think you had referred to a data warehousing company or a brokerage—how do you have an agreement with the primary entity through which the information is assigned and shared with the sub-entity? How do you compel production from the sub-entity when the sub-entity may not even be doing business in the same jurisdiction, or may not necessarily have the same moral obligations toward the use of the data? It has to occur near the top level, near the initial sharing of the data. If consumers choose to share information with other third-party sites, the means to compel the destruction of any data they share should be available at the avenue through which they share with the third party. It is difficult when it trees down like that to enforce production and destruction of user data.

[*Translation*]

The Chair: Thank you.

The last person to ask questions is Ms. Davidson. Go ahead. You have five minutes.

[*English*]

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

Thanks to each of you gentleman for being with us this afternoon. It's been a fascinating discussion.

I think we face a daunting task, and for many reasons. The speed at which the technology changes is certainly a challenge, as is the fact that we have very young children, plus older people like me, who get excited because they think they can use Facebook, not understanding a lot of the other things that go with it. Those are just two of the things that present a lot of challenges, I think.

I'm going to throw out a couple of questions and then I'll ask each of you to answer.

We've talked about not stifling innovation and how we want to see things progress. I think we're all in agreement with that. That poses a question as to how we can achieve a balance between preventive initiatives and legislative provisions to protect the users, realizing that legislation does take a lot of time in most instances.

My other concern is how we protect our young people. Mr. Elder, you talked about the Canadian Marketing Association and who you can market to and who you can't. How can that ever be regulated?

Mr. Péladeau, do you want to start?

Mr. Pierrôt Péladeau: As for the young people, I don't have specific expertise on that, so I cannot answer.

As for the issue of innovation, it can be oriented. Nevertheless, the existing data protection model, which dates back to the 1970s, still holds on. It's still solid. What we need is only to improve it.

That's why I have insisted in my presentation not to make what we're discussing something that is specifically targeted to some social media enterprise. What's happening is that this new environment reveals things that we can address. I think the most efficient way to address them is through a universal approach at the highest level, applying principles instead of specific procedures. In doing that, we can orient innovation rather than stifle it.

That's my basic answer. More specifically, we would have to look at specific issues.

● (1700)

Mr. David Elder: Again I would say certainly there's a balance that's possible, and I think we're very close to achieving it, as I said earlier. We have a principles-based approach. We have a Privacy Commissioner who is keeping track of technologies and new uses and consumer concerns as they go along. She's putting out guidelines. In many cases expectations are clear, I think, for companies as to what to expect. I think that is the best and most flexible model we can have.

In terms of marketing to children, frankly, I'm not sure there is an absolute, clear answer. Certainly the CMA has its code that says if you're going to collect information from those under 13 years, you need parental consent. I think the difficulty in legislating this—I don't know if this was part of the discussions in Washington, but in the U.S. they did legislate it. They had the Children's Online Privacy Protection Act. There were a lot of really bizarre and unintended consequences that came out of that act.

One of them was that a lot of sites just said that, because the rules were so difficult to comply with, they were not going to allow children under 13 to use them. Instead of taking an approach that might have had privacy protections appropriate to that age group that would allow the children to benefit from some of these social media networks, they shut out children completely, so children wound up lying or their parents lied for them. There were a number of problems. Another one was when they were getting parental consent they required some kind of identification, which tended to be credit card numbers, so they wound up collecting more sensitive personal information just to verify that they could use it.

I think the approach is there. The principle already says in the privacy legislation we have that you need knowledge and consent. I think that's already flexible enough and recognizes that it requires a different standard when you're talking to children.

Mrs. Patricia Davidson: Thank you.

Mr. Jason Zushman: With regard to your first question, Mrs. Davidson, I don't see why privacy protection and innovation can't both exist. I think you may even have technologies develop in relation to the provision of privacy and keeping information secure. Technology was a booming industry prior to the introduction of social media. Perhaps if legislation is empowered there won't necessarily be that same stifling of technology or that same sort of fear of that possibility.

In terms of protecting young people, I think what Mr. Elder mentions—codes that provide for the protection of children and underage users—are very beneficial. Perhaps education and public awareness programs that let kids know that the Internet isn't necessarily a safe place and that provide for different educational initiatives to help them realize that when you put something out there you're not necessarily getting it back and that it can have lasting consequences would be worthwhile initiatives.

Thank you.

Mrs. Patricia Davidson: Thank you.

[*Translation*]

The Chair: We're out of time. That brings today's testimony to an end.

Before we leave, I want to let you know that we had already discussed our next witnesses. So we gave ourselves until next Monday at noon to determine the witness list for upcoming meetings. We had already planned this week's meetings, but not after that.

Also, we could have a more specific directive on the study and the witnesses that every party would like to hear from going forward. We have until next Monday at noon. I would ask you to advise the clerk, as per the usual procedure.

Thank you everyone. Thank you witnesses, and perhaps we'll see you again.

Mr. Warkentin has something to say before we leave.

[*English*]

Mr. Chris Warkentin (Peace River, CPC): Thank you, Mr. Chair.

I just want some clarification. Parliament has determined that on November 8 we will have the Friday schedule so that people can get back to their ridings for Remembrance Day ceremonies that weekend. I'm wondering if there were any thoughts as to what we would do as a committee on November 8. My understanding is that most committees for that afternoon are being cancelled. I'm wondering what the will of the committee is or, Mr. Chair, whether you've given any thought to November 8.

[*Translation*]

The Chair: I serve the committee. If the committee would like to meet anyways, I will be there of course. I'm not sure if anyone else has something to add. It is certainly possible.

Mr. Angus, go ahead.

● (1705)

[*English*]

Mr. Charlie Angus: I think a precedent has already been set that if the House sees it as a day where the committee's not sitting, then the committee doesn't sit. That's what we've done in the past.

[*Translation*]

The Chair: That was my understanding as well. So we have consent not to hold a committee meeting on November 8. We'll follow a Friday schedule that day.

Again, I'd like to thank our witnesses. That brings today's meeting to an end. See you Thursday.

Meeting adjourned.

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

SPEAKER'S PERMISSION

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

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

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

PERMISSION DU PRÉSIDENT

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

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