HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 042 • 1st SESSION • 41st PARLIAMENT

EVIDENCE

Thursday, May 31, 2012

Chair

Mr. Pierre-Luc Dusseault

Standing Committee on Access to Information, Privacy and Ethics

Thursday, May 31, 2012

● (1100)

[*Translation*]

The Chair (Mr. Pierre-Luc Dusseault (Sherbrooke, NDP)): Good morning, everyone. Welcome to the second meeting of the committee in which we will hear from witnesses who will be speaking to our study on privacy and social media.

It is my pleasure to welcome Ms. Scassa, Mr. Geist and Ms. Steeves, all three from the University of Ottawa. They will each have 10 minutes in which to make a presentation. Then there will be a time for questions and answers about the presentations.

Without further delay, I will give the floor to whomever wishes to start.

Go ahead, Ms. Scassa.

Mrs. Teresa Scassa (Canada Research Chair Information Law, Faculty of Law, Common Law Section, University of Ottawa): Thank you very much for inviting me to speak to you today.

I will make my remarks in English, but I will be happy to answer questions in either English or French.

[*English*]

I'd like to begin by saying that I think it is very important that more attention be given to data protection and privacy in relation to the activities of social media companies. I do find it somewhat ironic that the committee's mandate was framed in terms of studying the efforts and measures taken by social media companies to protect the personal information of Canadians. It's a bit like studying the efforts made by foxes to protect the lives of chickens.

I note that to the extent that Google, Facebook and other social media companies attempt to protect the personal information of Canadians, these efforts have been shaped by data protection law. The adequacy of our data protection legislation must therefore be a focus of attention.

The amendments from the first five-year review in 2006 have yet to make it through Parliament; the second five-year review is already late in getting under way. These should be matters for concern, particularly since the data protection environment has changed substantially since the law was first enacted.

The current law is particularly weak with respect to enforcement. The commissioner has no order-making powers and lacks the ability to impose fines or other penalties in the case of particularly egregious conduct.

The focus on social media and privacy, in my view, has two broad aspects. The first relates to how individuals use these tools to communicate amongst themselves. In this regard we hear concerns about employers accessing Facebook pages, people posting the personal information of other people online, criminals exploiting Facebook information, and so on. These are concerns about the information that individuals have chosen to share, the consequences of that sharing, and the norms that should govern this new mode of interpersonal exchange.

The second aspect, and the one on which I'll focus my attention, is the role of these companies in harvesting or in facilitating the harvesting of massive amounts of information about us in order to track our online activity, consumption habits, and even patterns of movement. In this respect, attention given to large corporations such as Facebook and Google is important, but there are also many other players in the digital environment who are engaging in these practices.

The business models of social media companies are generally highly dependent on the personal data of their users. In fact, social networking, search engines, email and many other services are offered to us for free. By hosting our content and tracking our activities, these services are able to extract a significant volume of personal data. The nature and quality of this data is constantly enhanced by new innovations. For example, information about the location and movements of individuals is highly coveted personal information. More and more individuals carry with them location-enabled smart phones and they use these devices for social networking and other online activities. Even computer browsers are now location-enabled, and thus information about our location is routinely gathered in the course of ordinary Internet activities.

The point is that more and more data of increasingly varied kinds is being sought, collected, used, and disclosed. This data is compiled, matched, and mined in order to profile consumers for various purposes including targeted behavioural marketing. In some cases, this data may be shared with third party advertisers, with application developers, or with related companies. Even where the data is de-identified, its fine-textured nature may still leave individuals identifiable, as companies such as AOL and Netflix have learned the hard way.

Individuals may also still be identifiable from detailed profile information. The substantial volumes of information gathered about us make us highly vulnerable to data security breaches of all kinds. It's become very difficult to protect our personal data, particularly in contexts where privacy preferences are set once, and often by default, and the service is one that we use daily or even multiple times each day. Facebook or a search engine would an example of those.

It's often difficult to determine what information is being collected, how it's being shared and with whom. Privacy policies are often too long, too unclear, and too remote for anyone to actually read and understand. We now enter into a myriad of transactions every day and there simply isn't time or energy to properly manage our data. It's a bit like walking through a swamp and being surrounded by a cloud of mosquitoes. To avoid being bitten we can swat away; we can even use insect repellents or other devices, but in the end we're inevitably going to be bitten—often multiple times.

It's also becoming increasingly difficult to avoid entering this swamp. People use social media to keep family and friends close regardless of how far apart they live or because the social network communities have become a part of how their own peer groups communicate and interact. Increasingly, businesses, schools, and even governments are developing presences in social media, which give even more impetus to individuals to participate in these environments. Traditional information content providers are also moving to the Internet and to Facebook and Twitter, and are encouraging their readers, listeners, and viewers to access their news and other information online and in interactive formats. These tools are rapidly replacing traditional modes of communication.

● (1105)

To date, our main protection from the exploitation of our personal information in these contexts has been data protection law. Data protection laws are premised on the need to balance the privacy interests of consumers with the needs of businesses to collect and use personal data, but in the time since PIPEDA was enacted, this need has become a voracious hunger for more and more data, retained for longer and longer periods of time. The need for data has shifted from the information required to complete particular transactions or to maintain client relationships to a demand for data as a resource to be exploited. This shift risks gutting the consent model on which the legislation is based. This new paradigm deserves special attention and may require different legal norms and approaches.

Under the traditional data protection model, the goal was to enable consumers to make informed choices about their personal data. In the big data context, informed choices are very difficult to make. Beyond this, there is an element of servitude that is deeply disturbing. Nancy Obermeyer uses the term “volunteered geoslavery” to describe a context where location-enabled devices report on our movements to any number of companies without us necessarily being aware of this constant stream of data. She makes the point that equipping individuals with sensors that report on their activities leaves them vulnerable to dominance and exploitation—yet this is a growing reality in our everyday lives. Going beyond the simple collection of data, social networking services encourage users to make these sites the hub of their daily activities and communications.

Our personal data is a resource that businesses, large and small, regularly exploit. The data is used to profile us so as to define our consumption habits, to determine our suitability for insurance or other services, or to apply price discrimination in the delivery of wares or services. We become data subjects in the fullest sense of the word. There are few transactions or activities that do not leave a data trail.

As noted earlier, many so-called free services, such as social networking sites, document sharing sites, cool apps, and even Internet searching, are actually premised upon the ability to extract user information. In the 2011 decision of the Quebec Superior Court in St. Arnaud c. Facebook, a judge refused to certify a class action lawsuit against Facebook. To do so would have required classifying the terms of use for the site as a consumer contract so that Quebec law could override the clause that provided that all disputes would be settled under the laws of California and in California courts. The Quebec court found that there was no consumer contract because the Facebook service is entirely free, whereas a consumer contract is premised on payment and consideration. The judge found that there was no obligation placed on users that could be regarded as a form of consideration.

The case demonstrates how the provision of personal data is overlooked as an element of the contract between the company and the individual. It is treated as a matter governed by the tangential privacy policies. This lack of transparency regarding the quid pro quo makes it the consumer's sole responsibility to manage their personal information.

Concerns that excessive amounts of personal information are being collected can then be met by assertions that people simply don't care about privacy. To regard the sharing of personal data as part of a consumer contract for services, by contrast, places both competition law and consumer protection concerns much more squarely in the forefront. In my view, it is time to explicitly address these concerns.

Another social harm potentially posed by big data is, of course, discrimination. Oscar Gandy has written about this in his most recent book. We understand how racial profiling leads to injustice in the application of criminal laws. Profiling, whether it's based on race, sex, sexual orientation, religion, ethnicity, socio-economic status or other grounds, is a growing concern in how we are offered goods or services. Through big data, corporations develop profiles of our tastes and consumption habits. They channel these back to us in targeted advertising, recommendations, and special promotions. When we search for goods or services, we are presented first with those things that we are believed to want.

We are told that profiling is good because it means that we don't have to be inundated with marketing material for products or services that are of little interest. Yet there is also a flip side to profiling. It can be used to characterize individuals as unworthy of special discounts or promotional prices, unsuitable for credit or insurance, uninteresting as a market for particular kinds of products and services. Profiling can and will exclude some and privilege others.

I have argued that big data alters the data protection paradigm and that social networking services, along with many other free Internet services, are major players in this regard. To conclude my remarks, I would like to focus on the following key points.

First, the collection, use, and disclosure of personal information is no longer simply an issue of privacy, but also raises issues of consumer protection, competition law, and human rights, among others.

● (1110)

Second, the nature and volume of personal information collected from social media sites and other free Internet services goes well beyond transaction information and relates to the activities, relationships, preferences, interests, and location of individuals.

Third, data protection law reform is overdue and may now require a reconsideration or modification of the consent-based approach, particularly in contexts where personal data is treated as a resource and personal data collection extends to movements, activities, and interests.

Fourth, changes to PIPEDA should include greater powers of enforcement for data protection norms, which might include order-making powers and the power to levy fines or impose penalties in the case of egregious or repeated transgressions.

Those are my comments. Thank you very much.

[*Translation*]

The Chair: Thank you very much.

Mr. Geist, you have 10 minutes

[*English*]

Dr. Michael Geist (Canada Research Chair, Internet and E-commerce Law, University of Ottawa, As an Individual): Thank you very much.

Good morning. My name is Michael Geist. I am a law professor at the University of Ottawa, where I hold the Canada research chair in Internet and e-commerce law. I was a member of the national Task Force on Spam, and I currently serve on the Privacy Commissioner of Canada's expert advisory committee, but I appear before this committee today in a personal capacity representing only my own views.

My opening comments will identify several areas for potential government action, but I want to provide a bit of context with three key caveats.

First, which I think may be stating the obvious, is that social media is an enormously important and positive development. The number of users is staggering and its role as a key source for communication, community, and political activity grows by the day. The opportunities presented by social media should be embraced, not demonized, in my view, and government should be actively working to ensure that it incorporates social media into its policy consultation processes.

Second, Canada has played a leadership role, to a certain extent, in the use and regulation of social media. The Privacy Commissioner of Canada was the first to conduct a major privacy investigation into Facebook and has led on other issues with respect to social media and Internet companies.

Third, while we have had some influence through those investigations, Canada has not led in creating the social media services used by millions around the world. I believe that the failure to articulate and implement a national digital economy strategy comes back to haunt us in these circumstances, where the ability to place an unmistakable Canadian stamp on social media is undermined by the policy failures that have done little to encourage the development of Canadian e-commerce and social media.

With those caveats, what is there to be done? I'd like to focus on four areas of interest.

First, I think we need to finish what we've started.

The government has introduced and even passed legislation that can be helpful in addressing some of the concerns that arise from social media, yet these initiatives have stalled short of the finish line. Anti-spam legislation, for example, received royal assent in 2010, yet has still not taken effect as final regulations have not been approved. In fact, Industry Canada officials now indicate that it could be well into 2013 before the regulations take effect. Given the amount of work that went into this legislation, I find it shocking that it has been left in limbo.

Moreover, Bill C-12, the PIPEDA reform bill that seeks changes arising from the 2006 privacy review continues to lag in the House of Commons, with there frankly seeming to be no interest in moving forward with the bill. Indeed, I'd argue that the bill is even now outdated, and a full PIPEDA review to address emerging concerns such as order-making power—as you just heard—and damages, and tougher security breach requirements than those found in the bill is needed. In fact, the Bill C-12 security breach reporting rules are primarily bark with little bite, given the absence of penalties for failure to comply.

Successive governments have promised a digital economy strategy for years and have failed to deliver. The strategy has come to be known as the "Penske file", a reference to the *Seinfeld* episode that involves working on an imaginary file. While other countries are now years into implementing their strategies, in Canada we still lag behind.

I think it also should be noted that these issues must increasingly be addressed in concert with the provinces. The line between federal and provincial jurisdiction on many of these issues is blurry, and legal challenges against federal legislation is a real possibility. Work is needed to begin to develop minimum standards that can be implemented at the provincial level, should federal leadership be challenged in the courts by companies seeking to circumvent their privacy obligations.

Second, the devil is in the defaults. In many respects, social media and Internet companies are the most powerful decision-makers when it comes to privacy choices. As my colleague Professor Ian Kerr says, the devil is in the defaults. In other words, the choices made by leading social media companies with respect to default privacy settings are the de facto privacy choice for millions of users. Given the increasing pressure to generate revenues, we can expect that those default choices are going to change in more aggressive ways to make use of user data.

There are examples of companies that are doing good work in this area. Twitter recently implemented do-not-track options that won plaudits from the Federal Trade Commission in the United States. Google offers its users transparency tools so they can obtain detailed information about what information is collected, some of the ways Google uses it, and how they can modify some of their privacy choices. The company has also been transparent about law enforcement requests for information and copyright takedown demands.

There needs to be continued work on these defaults, as well as initiatives to provide users with greater information and transparency, and steps to ensure that companies live by their privacy commitments.

● (1115)

Third is the issue of lawful access. The introduction of Bill C-30 brought with it an avalanche of public outrage and concern over proposed Internet surveillance legislation. While much of the focus was on mandatory warrantless disclosure of subscriber information by telecom service providers, the potential for social media and big data Internet sites to serve much the same purpose cannot be overlooked.

A recent investigation by the Privacy Commissioner of Canada into Nexopia, a Canadian social network, identified hundreds of law-enforcement requests for customer name and address information, frequently for accounts that should have been deleted months earlier. Social media, as we've heard, generates a treasure trove of personal information that must enjoy full privacy protection and court oversight before disclosure. Indeed, documents that I recently obtained under access to information indicate that Public Safety is thinking about how these rules are applied to social media sites and services. I believe that Bill C-30 needs to go back to the drawing board to effectively account for these privacy concerns.

Fourth is the question of new legal issues, which Professor Scassa has identified a number of. I would argue that while much can be done to use or augment existing rules, social media and Internet sites do raise some unique issues that may require targeted responses. In the interest of time I would like to quickly identify two.

First is the issue of "do not track". As you may know, cookies can be used to trace the web-browsing habits of users, including when they visit third-party sites. For example, Facebook inserts a cookie on user browsers that traces your activity as you surf the Internet. Any site with nothing more than a Facebook "like" button, as found on Conservative, NDP, and Liberal websites, means that Facebook records a visit to that site and retains that information for months. A growing number of sites, including Yahoo, AOL, and Twitter, respect the functionality found in Firefox browsers that allows users to choose not to be tracked. Google has said it will implement similar technology in its Chrome browser.

However, many sites have been slow to adopt the do not track option, and Facebook has thus far declined to do so. Given the failure of the industry to self-regulate, it is appropriate for government to step in with stronger measures to ensure that this form of user choice is implemented and respected.

Second is the growing problem of social media misuse. For example, in recent months there has been an increasing number of stories of employers requiring employees to provide their Facebook user ID and password as a condition of a job interview. Seeking the same information with direct questions would typically be prohibited, so this is used to circumvent long-standing standards and principles within employment law. In response, the State of Maryland recently passed a law banning employers from requiring employees or job applicants to provide access to their personal digital and social media accounts. Several other states in the United States are working on similar legislation, and I believe that Canada should follow suit.

Thanks very much for your attention.

● (1120)

[*Translation*]

The Chair: Thank you, Mr. Geist.

Now we move to our last witness for today. Ms. Steeves, you have 10 minutes.

[*English*]

Dr. Valerie Steeves (Associate Professor, Department of Criminology, University of Ottawa): Thank you very much.

I'm the principal investigator of MediaSmart's Young Canadians in a Wired World research project. We've been collecting data about young people's experiences of online privacy for the past 12 years, which coincidentally means that we've been collecting data throughout the lifetime of PIPEDA. Over that time, we've tracked significant shifts that, I would suggest, provide important context for the work the committee has set out for itself. So I'd like to start my comments with a brief discussion of these shifts and then leave you with four specific recommendations.

In 2000, when PIPEDA came into force, the idea behind the legislation was that it would develop infrastructural mechanisms that would encourage people to have trust in e-commerce so that they would participate in this new form of wealth creation. When it came into force, we sat down and talked to parents and kids. The parents we talked to were very enthusiastic about this project. They had a lot of faith that the Internet was going to bring a lot of benefits to their children, and they felt that the companies that were developing these technologies were giving their kids tools to help them deepen their educational experience and also to help prepare them for the marketplace of the future.

They also told us that they trusted their kids when they went online to exercise good judgment. They weren't going to watch them all the time. They'd be in the background. They figured that their kids would make a few mistakes, but that when they kids got into trouble, they would come and say, “Hey, I need some help”. When we asked them if they would consider monitoring their children when they were online, they all told us, “Oh, no, that would be a breach of the trust between me and my child. If I did that, I would be invading my kid's privacy, so I would not do that”.

For their part, the kids we talked to in 2000 described the Internet as a completely private space. Adults couldn't even find it, let alone control it. They weren't worried about online privacy in 2000 because they were convinced that they had total anonymity when they were online. Interestingly enough, when they were deciding where to go when they were on the web, they looked for corporate brands because they felt that the companies that owned these brands were trustworthy. They were friends; they could trust them.

By 2004, for parents, certainly, the Internet had gone from being a panacea to a source of family conflict. They were aware their kids could release personal information online. They knew this was problematic. They had strict rules in the house, “Just don't do it”, but they spent an awful lot of time limiting, managing, and fighting over their kids' online activities.

The kids we talked to in 2004 had fully integrated online technologies into their personal lives, which I think underlines Professor Geist's introductory comments about the benefits of social media. These kids use this media and continue to use it to try on different identities, to deepen their connections to their real-world friends, and to follow their own interests. In 2004 they sometimes still did this anonymously, but most of the time they wanted to identify themselves because, contrary to popular opinion, they weren't talking to strangers. They were talking to the kids they went to school with and they needed to identify themselves so they could find their friends when they were online.

Even though they knew they could be watched, and they knew they were on so-called public media, online privacy was still incredibly important to these kids. I would suggest to you being very cautious about any claim that kids don't care about privacy because they post their lives on Facebook. Anyone who says that just hasn't taken the time to talk to kids; they care deeply about online privacy. It was becoming a growing concern for them in 2004, and in a follow-up survey of 5,500 Canadian school kids, about half of the kids we surveyed were beginning to notice that ads were popping up and were built into the places they went online.

Fast-forward to 2011. Now parents tell us that because kids go online through multiple points of entry or devices— laptops, computer labs, library networks, iPods, smart phones, iPads, gaming consoles—it's becoming increasingly difficult to supervise their kids' online activities. They also told us that it was highly problematic because they needed to supervise more because releasing personal information is now just taken for granted. You go online, because that's what you're expected to do. They were angry at online companies because from their point of view, these companies were encouraging their kids to disclose everything in order to make a profit. This resentment and lack of trust is a significant shift from 2000, when high-tech companies were seen to be building a future in which their kids would be empowered through technology.

● (1125)

Over that same time period, corporate sites, especially those sites targeting children, shifted from talking about privacy to talking about safety. It makes sense from the corporation's point of view, because when I'm talking about privacy, I'm the privacy risk because I'm collecting your information. If I'm talking about safety, I can tell you and your parents not to worry, because I'm keeping an eye out, I'm watching your child and I'll keep them safe.

Interestingly enough, almost all of the parents we talked to in 2011 were overwhelmed by this discourse of online danger. In fact, the sense of fear was so strong that they argued that good parents can no longer trust their kids and no longer exercise the benign neglect that was so common in 2000. And again, many of them blamed online corporations. As one Toronto parent said, “I really resent the fear that these companies have instilled in people.” All the parents said they were not even sure what the dangers were. All they know was that they're very afraid. They don't want to spy on their kids because that will hurt their relationship with them, but if they have to do it to keep them safe, they will spy on them.

For their part, the kids knew it. They told us that the unregulated private space they so enjoyed in 2000 and 2004 is now fully monitored, and they know it's fully monitored by parents, by schools, by their own peers, and by the corporations that own the sites they visit.

This puts kids in a very uncomfortable position, precisely because network technologies are so embedded into their social interactions. Interestingly enough, too, the kids said that all they needed was space to talk to their friends. They want parents and adults in the background, but they need privacy if they're to get the benefits of social interaction.

A number of them started talking about getting off Facebook and getting off their cell phones, because they were under so much surveillance. Interestingly enough, they all reported that the surveillance they experienced from all of those different people eroded the relationships of trust that are essential to their getting the help they need when they need it.

They're also beginning to question what will happen now that employers and police can get access to their Facebook profiles. They are also beginning to worry about what they called “the creepy people in the corporation who are watching them”. When you hear kids talk about creeps, creeping or being creepy, pay attention. That means somebody has overstepped the norms that are associated with exposure and have invaded their privacy.

It was particularly difficult when corporations did this, because when the 40-year-old creep sent you a message on Facebook, you simply blocked or un-friended him. The kids said “We can't do that with the corporations, because they own the sites we're on”. They also felt that privacy policies were written in totally incomprehensible language on purpose, precisely so companies wouldn't have to reveal what they were doing with their information.

Although kids still tend to congregate on corporate sites, like Facebook and YouTube, they no longer see online corporations as friendly or trustworthy. I think that's particularly important to keep in mind, because PIPEDA was designed to create that level of trust.

What can we do about it? How can we make it better? I have four suggestions for you.

First, I suggest that we need to increase the transparency of the business plans behind these sites. In 1999, when a number of us appeared before your predecessor committee, the government talked about PIPEDA being a floor and not a ceiling. As soon as it was passed, it quickly became the ceiling.

I would suggest that there's a great deal of empirical evidence out there that the consent mechanisms that we rely on and user license agreements and privacy policies are not being drafted to inform the individual so they can make choices about what they disclose; they're being drafted to protect the organization collecting the information from litigation.

In addition, it's becoming increasingly difficult to discover how that information is being used. I want to give you two very quick examples to illustrate that.

In 2000, I did a lot of research on a site called Neopets, which allows kids to create an online pet. They have to earn points on that site in order to buy their pet products and they would earn points by filling out market surveys.

In 2000, kids were asked to fill out a survey on breakfast food, for example, and in that context they were asked additional questions, like: How much money do your parents make? Do you have a big house? How many cars are in your family? What kind of cars do your parents drive? They were also asked to identify, off a list of 60 interests or things they might be interested in. The list included things like beer, liquor, cigars, cigarettes, and gambling. That information was then used to embed advertising into the site to encourage certain kinds of consumption.

I have some idea of the business plan behind that site. Since that time, because of concerns that were raised, both in Canada and the United States, those practices have become far less transparent. I can only get access to that kind of information now by snail mail and if I guarantee to them that I am a corporation. As a researcher, as a parent, and as a concerned citizen, I'm out of luck. I can't tell you what they're doing with the information.

● (1130)

It also has become much more difficult to see how this information is being used. Collection no longer occurs right in front of you. It occurs in the background. I got a friend request from Facebook, though I've never had a Facebook account. I have no relationship with this company. It said there was somebody called Melissa that I might want to be friends with, so I should join their network. I've never had a relationship with them, but they managed to track me to my daughter, even though we don't have the same last name, and even though she's never had a Facebook account either. I didn't release that information. I have no relationship with that company, and yet it is able to try to manipulate my behaviour through some business use that is non-transparent.

Second, I urge the committee to look not just at the use of personal information—

[*Translation*]

The Chair: Could I ask you to wrap up quickly by providing your last two recommendations?

[*English*]

Dr. Valerie Steeves: Okay, I'm almost done.

I urge the committee to look also at the uses of aggregate data, because that's how those profiles that Professor Scassa was talking about run. Personal information isn't the only privacy problem that we face online.

Third, I would suggest that section 3 of PIPEDA gives you an opportunity to find out about the purposes for which personal information and aggregate data are used by corporations.

Fourth, when we have these discussions the conclusion is often that we need more education. After working in privacy education for the last 18 years, I would suggest it is time that we started to take digital literacy education seriously. Right now, because the government is not supporting it, you're leaving it by default to corporations. We need to support public-interest organizations so they can provide people with the information they need to make intelligent choices and informed decisions on the Internet.

Thank you very much.

[*Translation*]

The Chair: Thank you very much. My thanks to the three witnesses.

We now move to a 10-minute question and answer period.

Mr. Angus, you may start.

[*English*]

Mr. Charlie Angus (Timmins—James Bay, NDP): Thank you very much, all three. This has been a fascinating discussion.

The New Democratic Party sees incredible democratic potential and social development possibilities through new media. The question is how to strike the balance. There are some disturbing elements that are happening in the world of Web 2.1 or 2.0, and we need to be careful. This is the thing. We don't want to overreach and interfere, but we want to ensure that protection is there.

Madam Scassa, I wanted to begin with the issue that you raised with PIPEDA, because this is our front line of defence. Our Privacy Commissioner has pointed out that Canada is falling farther and farther behind. We are becoming a laggard in basic privacy protections. I'm concerned about the breach reporting requirements. It seems that the potential rewrite of PIPEDA would allow the companies quite a bit of leeway in deciding whether or not to tell someone that their personal privacy has been breached. They talk about a serious risk. That is a pretty high bar. I can't imagine any company ever willingly telling their consumers that somebody has been hacking their data.

Do we need to have mandatory reporting? Would administrative monetary penalties ensure that these companies take the protection of personal data seriously?

Dr. Teresa Scassa: With respect to the two aspects, monetary penalities and data security breach notification, the concern with putting some boundaries on the obligation to report security breaches is that they're, unfortunately, so common and of so many different varieties that, if there were an automatic mandatory obligation to report every security breach, consumers would quickly become overwhelmed and even more distrustful of what corporations are doing with their data. There can be all kinds of issues or problems. Some middle ground was sought where only the more serious ones that really posed a risk to consumers or individuals would have to be reported.

There are different ways that you can do that. You can leave it to the corporation to determine the seriousness of the breach and whether or not they should be reporting it. Or you can have an obligation that corporations report breaches to the Privacy Commissioner and then decide, in consultation with the Privacy Commissioner, what steps should be taken to notify consumers. There can be a range of different types of notification or different types of responses.

I'm somewhat sympathetic to the concern about overwhelming consumers with information about breaches, but at the same time, I think there are ways to do it that won't leave the decision-making entirely in the hands of companies to determine when a breach presents a serious risk of harm.

The concept of serious risk of harm is a difficult one as well, just because it may not always be easy to assess what amounts to a serious risk of harm for individuals. I think that's going go be a difficult threshold.

As for administrative penalties, I think that would be an important weapon in the arsenal of the Privacy Commissioner. Not only does the administrative penalty impose a sanction on companies, which can be important in signalling that there has been a lapse in behaviour that is problematic and needs to be addressed, but it also has a more public shaming dimension as well. I think one of the concerns that's frequently been expressed about PIPEDA is that the commissioner has taken a very soft approach to dealing with corporations and doesn't name names, particularly in the context of most complaints, and so on, so that there's not enough information provided.

● (1135)

Mr. Charlie Angus: We're definitely feeling the need to allow the Privacy Commissioner to be the adjudicator, because an individual could certainly panic over any manner of breach without necessarily knowing the extent of it. The Privacy Commissioner certainly represents the public interest and has the ability.

Mr. Geist, I'm interested in this idea of our falling behind. Canada was a world leader in digital development. Six or seven years ago we had some of the highest penetration rates and access and speed. Now we look at the OECD standards and we're in the lower bottom third of the pack. We're looking at a paucity of vision of where we need to go with a broader digital strategy, in terms of democratic involvement, consumer rights, and economic initiative. Could you explain to us what your concerns are?

Dr. Michael Geist: Well, sure. This is an issue that I think most of our peer countries, most of the developed world, have identified as absolutely crucial to future long-term innovation and economic prosperity, as well as integral to what our education system, entertainment, and culture look like. It plays a role in so many different ways.

I think, as we've seen over the last number of months, whether through Bill C-30, or SOPA in the United States, or ACTA in Europe, the reality is that there's a very important political and participatory dimension here as well.

Unlike most other countries that have developed digital economy strategies, focusing on everything from ensuring widespread access to bridging the digital divide in terms of just basic access to computers, as well as the digital literacy and skills that Professor Steeves talked about, and the policy to ensure that we create the right framework to ensure that businesses start here and grow here, what we've seen in Canada is virtually nothing on that front.

In fact, there was a perfectly good consultation on this a couple of years ago when Industry Minister Clement was minister. There was a lot of feedback on it. We've seen a lot of other countries that have provided models we could look to, and yet there has been no digital economy strategy put forward. Few legislative initiatives have been put forward. I mentioned one, the anti-spam bill, but, 18 months after the bill received royal assent, there is still no finalization of the regulations themselves.

We've seen things like CAP, the community access program, eliminated during the most recent budget at the very time when there was at least an opportunity to look for some private sector leadership. In the United States you've got efforts between the government and large ISPs to provide low-cost computers, and low-cost broadband connectivity to ensure that the poorer parts of our society have access. We don't have any of that taking place in Canada.

So when you come into committee and you start asking what are some of the big policy issues that we have to grapple with, part of the problem is that you've got virtually no leading Canadian companies that are imbuing the kind of Canadian values that we're talking about in what they're doing.

You've got little leverage in trying to ensure compliance, because all of these companies are located outside of the jurisdiction. While that's not to say that you can't do anything—we've seen that there are some measures that can be taken—we'd be on far stronger ground, frankly, if we'd just get on with this issue of trying to set out a framework for the future.

● (1140)

[*Translation*]

The Chair: Thank you, Mr. Geist.

Your time is up, Mr. Angus.

Mr. Del Mastro has the floor for seven minutes.

[*English*]

Mr. Dean Del Mastro (Peterborough, CPC): Thank you, Mr. Chair.

Thank you to the witnesses. All the witnesses have given very interesting presentations today.

The Privacy Commissioner appeared on Tuesday and said that big data is the currency that Canadians are freely giving away without really understanding what it is that they're providing.

Professor Scassa, I believed you talked about companies harvesting information about us. I believe that was the term you used.

Professor Geist, you talked about default privacy settings and the devil being in the details.

Ms. Steeves, I'm actually very surprised that you could receive a friend's suggestion through your daughter with a different last name, and you've never been on Facebook.

Dr. Valerie Steeves: Yes.

Mr. Dean Del Mastro: It's pretty remarkably, actually. It demonstrates that there is a whole level of research and information being gathered that I don't think Canadians understand is being gathered. When the Privacy Commissioner talks about this currency that's being freely given away, and we talk about things like privacy settings and the default privacy settings that are going on, I don't think there's informed consent.

All of our witnesses today are professors of law who have a pretty good idea what it means when you read a disclaimer. Wouldn't it make sense if we started off with something that was very straightforward, and take the legalese out of it and say here's what you're signing up for, and if you don't want these things, click here? Wouldn't that be a good spot to start?

I'm interested in what you have to say about specifically informed consent. I think this idea of tracking is something that a lot of Canadians would find disturbing.

Dr. Valerie Steeves: Thanks.

Actually, I did some research that was funded by the Privacy Commissioner's office. The idea was to take kids to the privacy policies on a number of sites they frequented to see if they could understand them.

My research assistant is a 24-year-old. She's a university graduate, and she is working on a graduate degree. She called me up to ask if I could help her to understand what a privacy policy said. It took me about a day and a half, and I'm a lawyer. There were 17 links to 17 different sites. The language was contradictory; information was missing. It was a phenomenal experience. When kids say these things are really hard to understand, these really are hard to understand.

We took this to kids, and they came up with a set of strategies for plain language policies that they would find easy to understand. Then we looked at the literature and, ironically, the kids had come up with exactly the same thing that all of the academics had.

We rewrote the policies and then we empirically tested them. We did an experiment. We gave kids the original policies, where their comprehension was very low, and we gave them the rewritten policies, where their comprehension was very high. We published that. We have 10 best practices available to corporations in drafting privacy policies, but they have not been picked up.

Mr. Dean Del Mastro: Could you provide that to the committee?

Dr. Valerie Steeves: Definitely. It's available online.

Mr. Dean Del Mastro: Thank you.

Mr. Geist.

Dr. Michael Geist: I guess I'm of two minds on some of this stuff. There is no question that there is a necessity of ensuring that the kinds of choices and policies being put forward are better understood.

Quite candidly, I don't think any of these things are designed to be read, to begin with. Even if we did have better language, the reality is that given the number of sites people visit and interact with, and given the move towards mobile and wireless environments, the notion that people are going to sit and read the privacy policy before they engage in a website every time is unrealistic.

More realistic is to set in place some of the mechanisms, such as "do not track", to ensure that with the choices people would make, the reasonable person would likely say, "I'm quite comfortable providing you with a certain amount of information". It may be the case that they are not even aware of the implications of that, but let's take it as a given that a person who uploads a photograph or posts some of their likes or dislikes is doing so with some amount of knowledge it is being used and distributed to whatever circle they may have identified. We have concerns about how that may be misused and aggregated and the rest of it, but there is some amount of knowledge and choice there.

Then there are things around tracking your activity online. As I mentioned, literally all of your political parties have the "like" buttons. They have the tweet buttons to make it easy to retweet. We all like these things because they make it easy for us to tell our network. The reality is that every time you insert that on a website, it actually sends a message back without anything else. As long as you are logged into Facebook or Twitter—whatever the site happens to be—it is sending a message back to Facebook that the person has now visited that website.

I believe that kind of tracking activity goes well beyond the reasonable expectation of what a user expects. I frankly would be suspicious about any kind of plain language that would make it clear enough for a person to say, "Yes, this is what I would like you to do. As long as I happen to have some sort of Facebook widget included on the page, I would like you to track every website that I happen to visit for the next two months".

We need mechanisms to allow people to opt out of that more readily. We have seen some of those mechanisms, but too many of the large players have been reluctant to do so, because I think it runs counter to some of their business models. That's why there is a role for government to step up to the plate. If they are not willing to self-regulate appropriately, then government is going to do it for them.

● (1145)

Mr. Dean Del Mastro: Thank you.

Dr. Teresa Scassa: I agree with both sets of comments. The point to underline is that it's no longer just a transaction-based environment where we exchange personal information for a particular transaction. Many of us go online in the morning and stay online all day. We carry around smart phones; many of us have the location-enabled option on them for various reasons, which reports our movements.

It becomes a seamless thing. You have all of these different programs interacting with each other, and data being collected and shared in contexts where people are so used to using these different programs or applications, or interacting in certain ways, that to even go to the privacy policies is not a normal or automatic reaction.

Yet, things are happening that we're not aware of and that we might not consent to were we aware that they were taking place. I do think it changes the paradigm, and the legislation needs to respond to that.

Mr. Dean Del Mastro: Thank you.

I am—

The Chair: You can have a small question.

Mr. Dean Del Mastro: I am interested in this notion between aggregate and specific statistics. The use of aggregate statistics, it would seem to me, is basically what everybody is doing, and not necessarily interfering in the privacy of an individual. For example, if Google said that people with searches for this gave this as their top 10 responses, I don't see that as a privacy invasion. I see that as useful information.

When we get down to specific kinds of tracking, I think that's where most Canadians would be concerned.

Can you speak a little about the difference between aggregate tracking and specific tracking?

Dr. Valerie Steeves: Sure.

[*Translation*]

The Chair: I will allow one person to answer quite quickly.

[*English*]

Dr. Valerie Steeves: Okay. When you use this data, you're collecting all this personal information. You're tracking population trends. Then you divide everybody up into categories, and then you treat them differently because they belong to a category. Earlier a concern was raised that this type of technology is very important for democratic debate. You can use those categories, once people identify themselves, to change the environment around them.

I was doing research on MSN, and while I had not identified myself as any particular person, I was surrounded by the news of the day. As soon as I registered as a 16-year-old girl living in Vancouver —which I was not, as you might have guessed—the news of the day disappeared and it was replaced with celebrity news, dieting ads, and plastic surgery ads. It wasn't that they knew I was Val the 16-year-old girl living in Vancouver; they knew I was someone who fit that category.

Therefore, there are issues of discrimination that flow from that, as Professor Scassa mentioned, but they are even more insidious, because they change the environment around a person because of their assumptions about who they are and what category they fit into. So that would not fall within PIPEDA protections on the use of personal information, but it's highly problematic from a privacy point of view, because it fractures the public spaces that are necessary for democratic debate, and it opens up vulnerable populations to discrimination.

[*Translation*]

The Chair: Thank you.

Your time is up, Mr. Del Mastro.

Ms. Murray, you have seven minutes.

[*English*]

Ms. Joyce Murray (Vancouver Quadra, Lib.): Thank you very much for presenting to the committee your ideas about what should be done.

What struck me when I was listening to you was that in some ways Canada is falling behind. At the same time, given some of the budget cuts, other organizations are impeded from helping to slow down that falling behind.

With the incredible complexity of what you've just presented and the potential for different interest groups to have different ideas about how to move forward, I'd like you to comment on whether the tools we as government have in the form of laws and enabling those laws and regulations are up to the challenge when we have such a fast-paced and dynamic environment. Or, is it the case that what we're trying to bring to bear as Parliament and government just has to be totally rethought if we are to catch up and do something that is in real time with respect to the risks and the concerns? It's a pretty broad question.

● (1150)

Dr. Teresa Scassa: Yes, it is a very challenging environment. One of the things I talked about—and I think Professor Geist mentioned this as well—is that the problems are now so multi-dimensional and complex that it may be the case that they simply can't be slotted into one particular box of data protection legislation under federal jurisdiction. It may be that there are other dimensions that implicate other regimes, whether it's competition law or human rights law, or that implicate the provinces as well. So it may be that there's a need for a more multidisciplinary, multi-faceted approach to some of these issues, and that it's not necessarily to our advantage to treat or deal with the issues in specific silos.

Dr. Michael Geist: I have a couple thoughts on that. The first is to say that I don't think it's the role of government to come charging in saying, "We're the new sheriff in town when it comes to social media, and we're going to fix everything that has to do with the choices these private companies and individuals are making".

Frankly it's tough to keep pace with what's happening. As we've heard, we're not even sure, necessarily, what the business models are sometimes. We don't know if there is a business model in some of these instances. So I think taking the approach that government knows and is going to fix everything would be foolish. That said, there is unquestionably a role for government and regulators to set certain parameters about what is appropriate and to ensure that it reflects Canadian values about what's right from a privacy perspective and what's right in terms of an obligation from a security perspective, as well as about the range of different issues that arise.

In that context, I find I'm a bit more optimistic about the prospect that government can engage in that broad rule-setting. PIPEDA, in many respects, was designed, at least initially, with the best of intentions to try to do just that. As Professor Steeves noted, we've now had more than 10 years of experience, and that experience has shown that there is a need for adaptation of the law. So it's not that we're changing something every 10 weeks. But surely every 10 years is enough time to say that there are shortcomings within the legislation on the privacy side that we can fix to ensure that the sorts of broad parameters around some of this activity better reflect what Canadians expect when they venture online.

Ms. Joyce Murray: I have another, associated question. Perhaps, Professor Steeves, you could wind your remarks into both of them.

It was mentioned that they were trying to find a balance between privacy and access to data, and how critical this was for business and the competitive issues that come up. I'd like to have positive and negative comments about the impact on small businesses—not the big data businesses—of what's going on.

I'd also like to know whether there is a country that has a framework for addressing these issues that could be a suitable model for Canada, or whether it's about unique values and principles in Canada and that we must have a made-in-Canada approach.

Dr. Valerie Steeves: As was mentioned earlier, online privacy issues are really nested in broader concerns about marketing, citizenship, human rights, social interaction, democracy, democratic dialogue, and those types of things. If you go back to the history of data protection, it was always assumed that it would be the last step. That's the floor, not the ceiling, approach. It was assumed that there would be mechanisms whereby governments would interrogate uses of information and ask if the public interest were served by these practices. If it were, only then will we go ahead with that kind of thing. We'll use fair information practices once the horse is out of the barn, to provide some redress in case something happens.

I think the reliance on fair information practices perhaps reflects a naivety that it will be enough. It might be a necessary but insufficient condition.

I would suggest that the jurisdictions that have approached these issues from a broader perspective and come up with solutions that better capture these broader human rights interests are places in Europe, for example, which have a human rights approach to privacy and where there are strong human rights protections for privacy, for the inviolability of the personality. There are a number of situations in Iceland and Germany where courts have been able to come up with creative solutions, interrogate those purposes, and call those purposes to some form of public judgment through broader understandings.

I agree with what Professor Geist said about consent. Consent is never going to be your solution. I think it's an important piece of the puzzle, but it's a small piece. We need another mechanism to interrogate these broader purposes. That's why I pointed you to section 3 of PIPEDA.

It was argued before in your predecessor committee that we needed section 3 because that way, you could look at purposes and say that it's not something a reasonable person would consider appropriate under the circumstances. And if it's not, then you shouldn't be doing it. There's quite a power on your part because of that provision to think more carefully about restricting certain uses of information.

● (1155)

Dr. Michael Geist: Often the question is put: Who does it better, or who does it best, and can we emulate them?

When PIPEDA was first established I think there was a view among many that it was the best practice. It looked at a lot of what was taking place in Europe and at what had emerged in the United States. In many ways, it tried to bridge the two different approaches. There can be disagreement over whether there could have been some tinkering here or there, but it genuinely tried to do that.

A number of countries looked to Canada as a model for how, on the one hand, to respect some of the views on privacy that have come out of Europe and at the same time to reflect some of the business considerations and enforcement elements that we've seen in the United States.

I would say that over the last 10 years we've really fallen behind. We've seen Europe, in some ways, get more aggressive on some of these issues, and we haven't kept pace. We've seen the U.S., frankly, do a far better job on the enforcement side than we have. There are real penalties there. If you screw up from a privacy perspective in the United States, you're going to pay. They are also the ones that came up with mandatory security breach disclosure requirements, which we see in States everywhere. We're seeing it, as I mentioned, in moving toward “do not track”. We're seeing it with respect to the misuse of social media, which I referenced as well.

I think it's about picking and choosing some of the very best that we've seen, from an enforcement perspective in the United States and from a values perspective from what we see elsewhere, to create an environment where we're not saying that we're like them but that we want other countries saying that they're like Canada. Over the last decade, we've failed to identify what it means to ensure that we have a privacy legislation that keeps pace with this changing world.

[*Translation*]

The Chair: Thank you.

Your time is up, Ms. Murray.

Mr. Butt has the floor for seven minutes.

[*English*]

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

Thank you all for being here today. I found your three presentations to be just excellent.

My daughters are 12 and 8. My 12-year-old daughter has decided that she, unlike Mr. Angus, likes Twitter. She has decided to set up her own little Twitter account and she does text, mainly to her little school chums.

As a parent, I am concerned about whether there's private information that is going to be accessed in some way, shape, or form.

Are you of the view that we can, or should, be looking at privacy measures for minors in a different way than we would for adults? Should we make the assumption that adults should know better? Adults are adults, and they should be smarter and should know better.

Should we look at strengthening privacy provisions to protect minors who are users of social media, or should we, in your view, treat everybody the same, regardless of their age?

Dr. Teresa Scassa: Maybe Val could start.

Dr. Valerie Steeves: Sure, I'll take that one.

There were recommendations with the first PIPEDA review to have a tiered consent mechanism that recognized differences in ages. The suggestion was that under a certain age, companies shouldn't be able to collect any information at all. Then as kids become older, they can opt into programs where they can say the companies can have that information and can flash them a few ads. But it put real restrictions on what they would be able to do. Probably most importantly, there was a suggestion that once somebody turned 18, there should be a big delete button so that the information was forgotten.

If you look at how kids use technology, they use it to meet their developmental needs. When you talk to 11-year-olds, younger kids, they're actually the ones who make me the most comfortable. They sound the most mature. They say that they don't do any of the social networking stuff, certainly not in the broad world, because that's for older kids. They're very aware of the risks, and they manage them quite well.

When they hit 13 and 14, they're at a different developmental stage. They're exploring their identities through performance. They tend to do outrageous things, writ large, for a couple of years.

Then when they hit 15 to 17, right up to the early 20s, they explore their identities through social networks. If you think of it from their point of view, these technologies are fabulous, because they give them an opportunity to meet their needs as they become individuals and grow to be adults.

I certainly would not want to have to look at anything I wrote when I was 14 in any kind of public environment. Certainly for kids, yes, I think you need a forget button. There is definitely something different when you're a minor.

One of the interesting things that's come out of the research is that there was this belief that these digital natives would be different from us. Ironically, when they hit about 29, they start acting just like you and me, and they use technology the same way we do. They grow up, in other words.

So yes, they are different. I share the same concerns about using consent as a mechanism to provide that protection, because you have to identify an age for that system to work.

I was launching some research yesterday with a youth panel, and an 11-year-old told CBC all about how all of his 11-year-old friends in grade 6 have Facebook accounts. They know that they're supposed to be 13, but they just click the right button. I think we do a disservice to kids if we say that we have to put them under surveillance to make sure that they're old enough. That won't help. Certainly, having broader restrictions that say that kids are kids, so don't collect their information, and when they get older, don't use it in particular ways....

There was the Nexopia complaint, for example. Nexopia was the most popular social networking site for kids. One of the commissioner's recommendations was that they not retain information over a certain period of time. Nexopia just said, “Sorry, we're keeping it. There's a lot of money in this stuff”. You're talking about 12-, 13-, and 14-year-old kids.

The other thing is the use the information is put to. I don't have time to go into any details, but I can point to some research we're doing with young girls. The site is embedded with marketing material that uses very stereotypical images, particularly for gender. I've just done some really fascinating qualitative research with young women. They talk about how this restricts what they can do, and they're constantly trying to force it back. It's actually narrowing the kinds of people they can be rather than broadening the world for them.

Yes, we do have to think about kids differently. I think the way to do that is to look at the uses of the information and just say that it's not reasonable to collect information from eight-year-olds and then use it to try to sell them anything.

● (1200)

Mr. Brad Butt: Go on.

Dr. Michael Geist: Professor Steeves is the expert in this area, so I hate to take a different position. But I have to say that we've seen an attempt to try to target kids, from a privacy perspective, in the United States, with COPPA, the Children's Online Privacy Protection Act, which sought to have specific protections, and, essentially, parental oversight and consent for kids under 13. This legislation is a joke.

My kids are actually similar in age to yours, although I have one more. They're in this world as well. The notion that a company would say, “Hold on a second, we're not going to collect any of that information until we get your parents' consent. We're not going to collect anything at all...”.

The truth is, there are peer pressures. There's a desire to be there. Frankly, there's an awful lot of good that comes from this environment as well.

The idea that we can set specific rules that say that they're simply not going to collect or that they're going to get stronger consent we've seen for almost 10 years. There was a legislative attempt in the United States. I think it fails miserably, because the kids are smart enough to know that they can get around it if they want, and the companies will just look the other way as they know that it's happening.

From my perspective on these issues, we need tough standards that are enforceable. We need real order-making power from the Privacy Commissioner's perspective, with the potential for penalities when people overstep. And it would apply to all.

Mr. Brad Butt: Thank you.

I'm sure my time must be up. That must be five minutes.

The Chair: You have one minute.

Mr. Brad Butt: That was the main question I wanted to ask. If someone else wants to take the extra minute, I'm leaving the committee anyway.

Mr. Blaine Calkins (Wetaskiwin, CPC): Sure, I will go.

Mr. Geist, I was listening to your questions a little while ago. One of your comments was about a reasonable expectation that users might have of how their personal information might be treated. That sounded like a legal definition. Is that defined anywhere in the current legislation? Does it need to be defined, or is the definition outdated? Is it outdated in PIPEDA? Is it a case law definition?

It sounded to me that this was some kind of standard verbiage that is used in the industry, and I'd like some more clarification on that.

● (1205)

Dr. Michael Geist: It is common language that they use, and I think it's highly problematic language. It's true that I used it, but there is a problem with relying on a reasonable expectation of privacy—which you actually see crop up very regularly in labour cases and other sorts of cases where they talk about what someone can reasonably expect. If there are privacy policies saying you shouldn't expect any sort of privacy, and if you have received clear notifications that they're going to collect all the information they can about you and will do absolutely everything they can to try to monetize it—they typically don't put it in that straightforward language, though that is essentially what they are often saying—then when you ask about what your reasonable expectation of privacy should be, the response is akin to the infamous Sun Microsystems' response, “You have no privacy. Get over it”. In that case, you have no reasonable expectation of privacy because you were told that you didn't have any, so get over it.

So in setting appropriate boundaries and standards and ensuring that we have effective tools to enforce those, we get away from the paradigm of saying, “You only get what you expect, and you shouldn't expect everything”, to saying “No, there are some minimum standards about what's appropriate and we have the tools to ensure that they're there and that they're going to be enforced”.

[*Translation*]

The Chair: Thank you.

Ms. Borg has the floor for a five-minute question and answer period.

Ms. Charmaine Borg (Terrebonne—Blainville, NDP): Thank you very much.

I would also like to thank the witnesses for coming here today. The testimony we have heard is interesting; we are opening a Pandora's box of issues and questions.

My first question goes to Ms. Steeves.

You said that when you registered as a 16-year-old girl, you got advertisements specifically targeted to 16-year-old girls. Can you tell what effect advertising on social networks has on the behaviour of those young users?

[*English*]

Dr. Valerie Steeves: One of the problems with answering that question is the lack of transparency. I would like a lot more information about the business plan behind these sites—and certainly describing how the back engine works—and then I would feel more comfortable in responding.

What I can tell you is what we know about the front engine. There's a lot of research that tracks how people respond to media images around gender, for example. Perhaps the best explanation would be to look at some of the work coming out of our eGirls project, another research project I've been involved in. Young women are telling us that when they're on these sites, they're surrounded by particular images of very thin, highly sexualized young women who are identified primarily through a relationship with a male. For background for our work on that project, we started with an environmental scan. We looked at 1,500 public profiles on Facebook of girls who ostensibly live in the Ottawa area. Those were public profiles. We didn't look at private profiles.

Now, of those 1,500, every single one we looked at, with one outlier, reproduced that stereotypical image of gender: highly sexualized young women, with the pouty faces and the bikini shots, with all the talk being about the boyfriend.

Now, there aren't any quantitative studies indicating there's a causal relationship between marketing and behaviour like that. There's an assumption, certainly on the part of marketing companies, that the reason these marketing images are used is so that they can steer behaviour, which they appear to be quite successful at doing. What we do know from talking to young people who live in these environments is that these very stereotypical images get in the way. For the young women who embraced them and sought to emulate them, they were wistful, in the sense that, “Gee, I just can't do it that well. No matter how much I diet, I'll never be that skinny”. For the women who wanted to be someone else, they said they constantly had to negotiate with these images and push back against them. That's driven by the marketing message they're getting.

One of the things that's interesting about the trajectory of what's happened in Canada—and Michael is right that we used to be leaders in all sorts of areas—is how well we did with Canada's SchoolNet. We provided public spaces where kids could talk to each other, spaces that weren't commodified, that weren't commercialized. The federal government got out of that business shortly after PIPEDA was passed. By default, what we're seeing is a lot of organizations that have kids' best interests in mind are using corporate sites to do things.

For example, a lot of schools—and we did a lot of work on this with teachers recently—are telling us they use Google Docs. There's no acknowledgement that that information can even be collected and used and reshaped to manipulate the kids who use that particular platform. Frankly, I don't think my kids should doing their homework in a store, you know?

I think the way behavioural marketing and advertising actually works is that it doesn't look like advertising. So if you talk to kids and you ask them what Facebook is, they tell you it's a social network. It's not a social network; it's a research lab. It's designed to collect information about people so it can be used and marketed back to them.

It's highly effective. We have definitely seen shifts—certainly in my research—about the way that kids respond to these particular images. I'd point you to all the research coming out about body image problems, and the increased use of cutting. There are all sorts of consequences. In this regard, I was at a meeting in Edmonton recently, where a number of doctors and academics got together because we see this as a health issue.

● (1210)

[*Translation*]

Ms. Charmaine Borg: Thank you. I am sorry; I do not have much time left and I want to ask you another question. But I do see the extent to which privatization is reducing the public space on the Internet. I find that very worrying.

Here is my last question, Ms. Scassa. You said that people are talking in terms of security and not talking specifically about personal information. In your view, how does that change the relationship between the Internet user and the social media companies?

The Chair: You have about a minute to answer the question.

Mrs. Teresa Scassa: I am not sure that I understand the question. Are you talking about security?

Ms. Charmaine Borg: The discussion is all about security and cybercrime instead of being focused on personal information. I am asking what that semantic change would mean.

Mrs. Teresa Scassa: Certainly there is a lot of concern about personal information being lost from companies of this kind and the repercussions that has on us, whether in terms of identity theft or of criminal activity on the Internet.

Legislation dealing with the protection of personal information is still based on personal information. I really feel that we are losing the meaning of that concept, of what personal information is. We recognize that it means a name, an address and other information that you might give to someone. But more and more, personal information is information about all our activities, about everything we do online, and even elsewhere.

Given that, I think that we have to focus on the entire body of personal information that we share with companies to a greater and greater extent. I don't know if that answers your question.

The Chair: Thank you.

Ms. Borg, your time is up.

So Mr. Mayes now has the floor for five minutes.

[*English*]

Mr. Colin Mayes (Okanagan—Shuswap, CPC): Thank you, Mr. Chair, and my thanks to the witnesses. I really appreciated your input here this afternoon.

Mr. Geist, you mentioned Canadian values. As to privacy, I see this as drawing a line in the sand. What privacy is to me could be different to others. There's consent, but is there a user-specific consent where I'm willing to go so far and no further, a consent that I have to define for myself? That's the challenge I see in putting regulations together. Where do you pick up those Canadian values? That term means different things to different people. Could you develop that a little bit for me?

Dr. Michael Geist: You're right that many people have different perspectives on some of these issues. I think there's some low-hanging fruit here. We could start by ensuring that there's respect for people's choices about consent and that there's adequate disclosure from the organizations collecting the information. It is important to have informed consent.

We need to move further along that chain. I think it's fair to say that at the moment Canadian law doesn't do a good enough job. We don't get the disclosure where there are security breaches with any sort of penalties. We don't have order-making power to ensure appropriate compliance. And we don't have penalties where there is insufficient compliance. At present if a company doesn't like what the Privacy Commissioner of Canada has said, they just tell them to go to court, that they're not going to abide by the decision. At the provincial level, we have commissioners with order-making power and the ability to enforce.

It's pretty tough to have faith in the Privacy Commissioner's ability to represent the public interest, to enforce the values that are broadly reflected within society. The commissioner has told you that she can't do her job—the legislation, which dates back more than a decade, doesn't give her adequate means of enforcement and organizations are increasingly willing to push back.

There is concern about the blurriness between federal and provincial jurisdiction. But in light of the securities regulation decision from the Supreme Court of Canada last December, I think we'll see that, absent some real changes in the law, if the federal commissioner tries to get aggressive about enforcing the rules, any company that doesn't like what the commissioner has done will say, "Go sue me." They're going to tie it up in the courts for years. And there is a clear risk that the courts may say no, or find the law itself to be unconstitutional. I think if we did nothing more than try to ensure appropriate disclosure and adequate enforcement of consent, we'd be miles from where we are right now, given some of the shortcomings we see in the law.

● (1215)

Mr. Colin Mayes: That's an area I'm interested in—enforcement. It's like a barking dog chasing a car. Are you ever going to catch up to the technology and the ways it's used? That's a challenge.

Mrs. Scassa, will enforcement proceed on a complaint basis? How do you deal with these corporations and track them? The cost of having people do that is phenomenal. Is it only on a complaint basis that you can react to this? Could you give me some ideas on enforcement of the regulations that we manage to put together here?

Dr. Teresa Scassa: There currently is a complaints mechanism under PIPEDA, but there is also the possibility that the commissioner can conduct audits of the information practices of companies, and she has done so on a number of occasions. There are a number of different powers you can give to a commissioner, whether it would be audit-making powers or a complaints-based process, including the possibility of initiating a hearing or a process where there appears to be a problem, on her own initiative, for example.

There are a number of different ways in which you can do it that don't necessarily make it completely complaints-driven. There are problems with complaints-driven mechanisms, because they make you respond to the things that people are bringing forward and, as you mentioned, they may involve a significant cost burden. Certainly, the volume of complaints has increased over the years, so there are other ways in which the commissioner can be given powers to react.

We've talked already about the power to issue fines, for example, or to take extraordinary measures in specific cases. I think the menu of options is quite broad and there can be multiple options in any piece of legislation; there can be a range of different powers, depending on the circumstances and depending on the particular norm or concern.

[*Translation*]

The Chair: Thank you.

Unfortunately, your time is up, Mr. Mayes.

Mr. Boulerice, you have five minutes.

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

I would like to take a few moments to thank you for being here and also for the quality of your presentations and your answers. This is really a very interesting meeting. The subject is fascinating and your comments make it all the more relevant.

A number of years ago, I was struck, as many are, by George Orwell's novel *1984*. In the novel, the all-powerful government takes on the form of Big Brother watching over people's lives. The picture you are painting gives us the impression that the government could actually be a Big Brother. When the Conservatives introduce a bill like Bill C-30, we get chills up our spines, and with good reason.

But my impression is that we have a whole lot of "Medium Brothers" in the form of large Internet companies. They are getting to know our lives, to watch us, to know what we like and do not like, what we buy and do not buy, what interests us and what does not. Then they can go into action.

Is it your impression that online social media have become a bunch of Big Brothers?

● (1220)

Mrs. Teresa Scassa: Along with the George Orwell novel, you also hear the Tom Cruise movie *Minority Report* mentioned. In that movie, you see commercials changing according to the person watching. Yes, I think we are watched by companies more and more. But you also have to realize that the information they gather about our activities and habits, our location and our movements, is also available to the government.

For example, provisions in the Personal Information Protection and Electronic Documents Act give companies the ability to share information without obtaining consent in connection with a lawsuit or an investigation by the authorities. That is becoming more and more frequent. My colleague Professor Geist mentioned it. We are watched by companies and the government has access to the same information. That really is worth taking into account.

Mr. Alexandre Boulerice: Thank you.

Does anyone else want to comment?

[*English*]

Dr. Michael Geist: Sure. I want to harken back to the very first caveat and that is to emphasize how important and valuable these services are.

I recognize the language around big brother and social media, but I have to say that the value that's associated with this for so many different purposes, from community to activism to culture to education, is very important in a way that if we started calling this big brother, it would clearly put a negative spin on it.

I do think Professor Scassa's point is absolutely crucial, and that's one of the reason I referenced it in my opening remarks. Ten years ago, the big fear among many in the privacy community was about countries like the United States creating these large, all-knowing databases. They went by terms like Echelon or Carnivore or Total Information Awareness, TIA. I don't think the government, to the best of our knowledge, was ever able to create that in the United States. But databases much like those have effectively been created by the private sector, as many of us have actively given up that information to those companies, who, in many instances, as I mentioned, have obtained real value out of it.

The danger we face is that the kinds of limits that we have in legislation, within the Privacy Act, for example, which might set limits on what government can do with the information it collects, have not been established in the same way for information collected by the private sector and then accessed by government. Effectively, it is a circumvention or an end-run around the very rules that government has imposed on itself, to allow law enforcement and others to collect from third parties and do with that information what they are legally or otherwise unable to collect or do.

[*Translation*]

Mr. Alexandre Boulerice: Thank you; the clock is ticking.

I have nothing against social media. I love Facebook and Twitter. They let me keep up with the news incredibly well and to share videos, information, and people's photographs.

I would like to ask you a quick question about the business model. A few years ago, an executive of TV1, a private television channel in France, said that he was selling available human brain time to Coca-Cola. He meant that his job was to get viewers to watch commercials. It is just like buying a paper. You think that you are buying the articles, but you are not; you are selling yourself to the newspaper's advertisers.

Basically, we can use and love Facebook, Twitter and Google all we like, people have to realize that they are voluntarily giving their private information to a company that will subsequently turn around and sell that information to other companies that will model and target the advertising that will then be sent back to the people. Is that right?

● (1225)

[*English*]

Dr. Michael Geist: Well, I think absolutely. As far as we know, the business model for many of these companies—and I think that for many of them, they are evolving, shall we say—is to leverage the information, the social graph that they're able to accumulate, and add value to that for marketers or others. There's no question that that's the model. That isn't, in my view, bad per se. There is a lot of value that comes out of this environment.

The danger comes where we engage in, as I talked about earlier, things like social media misuse, or the collection of information that I think in many ways feels somewhat surreptitious, where people are unaware of what's taking place. They're being tracked in ways that aren't providing information in the way that we typically think of, such as entering a bunch of fields on a computer screen, or uploading some pictures and saying, “Here this is”. In fact, it's the other kinds of activities that are actively being tracked and used, in much the same way that you've just described.

[*Translation*]

The Chair: Thank you.

Unfortunately, your time is up.

I now give the floor to Mr. Dreeshen, who has five minutes.

[*English*]

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

Thank you so much for coming today.

I was watching a television ad just a short time ago in which someone had been able, with their cellphone, to look at the speech that was being presented by a coach as he was talking to his teammates. He talked about how great it was that he was able to just move that thing down to YouTube and bring it right into the school so they could cheer them on. But here I think of what you mentioned just a few moments ago about the misuse of social media. Obviously they looked at it from that perspective of saying, “Isn't this great?”, but I think you're taking a look at the other side of it as well.

I was a schoolteacher for many years. Thinking back to when I went to university, it was always nice to be able to get somebody else's notes, if you didn't make it to class or whatever. But here it's just a case of “Why don't you just tape what's going on?”, and you can send it to your friends. Then I started looking at the propriety of what is being produced by the instructor and all of these other types of things and the types of protection you have.

That may or may not be associated with the privacy issues we're speaking of today, but nevertheless, it's one of those kinds of things that people have to be aware of. This means that institutions have to start bringing up certain rules in schools, where they say that you're not going to be able to go on Facebook or you're not going to be able to bring your cellphones or anything else into the classroom.

Those are the kinds of things I see. So when we try to bring some policy and some thoughts together on this, I think your comments on that would be something that I'd appreciate.

Dr. Valerie Steeves: As part of the young Canadians project, we talked to 10 key informant teachers across the country, so I actually have good data on this. They perceive it as a privacy issue, because when the walls of the classroom become transparent, you lose the ability to create a safe space where kids can make mistakes, explore, and learn, effectively. In addition, there are all sorts of problems that happen when kids surreptitiously take tapes of what is happening in the classroom and post them online. It changes the dynamic significantly.

Uniformly, the teachers we talked to all indicate that the solution was not to get rid of the technology. In fact, that has been our knee-jerk reaction—"Oh, we don't like this, so let's just shut it down". Social networking and these types of tools can really deepen kids' education, and I have a report of incredible best practices to justify that.

However, what they told us is that the real problem is that the schools are taking this approach and they're banning things. If they do allow kids to go online, they place them under total surveillance. By doing that, they also place the teachers under surveillance. What that does is shut down the opportunity to be that caring adult beside the kid when they do run into trouble or when they say, "Hey, this looks like a kind of a wingy site", and the teacher can go over and go, "Yes, that's a hate site".

So those teachable moments where we can give kids true digital literacy skills are shut down by not embracing the technology. But at the same time, I would stress that it is a privacy issue.

Dr. Michael Geist: I see the use of these tools, particularly for education purposes, as having a tremendous amount of potential. For instance, this particular hearing is not only being viewed; I took a quick glance, and there are also people tweeting about it as they listen or watch it in real time. The classroom isn't just the classroom that we tend to think of at, say, the University of Ottawa. This is, in a sense, a classroom, where others have the opportunity to watch, to listen, to interact, and to engage.

So I think there are great opportunities there. One of the things the government ought to be thinking about in there is how we can better facilitate the use of these sorts of tools and technologies to bring the educational opportunities to as many people as possible.

For example, Bill C-11, the copyright bill, did some of those things, but at the same time, there are distance learning provisions in there that require, as you may know, teachers to destroy lessons that are used under that particular exception within 30 days. To me, that's a most unfortunate provision in there, one that I think actually shifts us in the wrong direction when we start talking about the way we use these tools in furtherance of ensuring better education, better educational opportunities, and, frankly, ensuring that more people have access to this, not less.

● (1230)

Mr. Earl Dreeshen: Ms. Scassa.

Dr. Teresa Scassa: I would agree with that. I think there is enormous potential for creativity, for dynamism, for reaching learners with different styles and different abilities, and for bringing information and resources to the classrooms. There is tremendous potential there.

What I see, and this is purely on an anecdotal basis as a parent, is not a lot of guidance coming from the schools, not a lot of information. My 10-year-old daughter brought home an acceptable computing use form that she had to sign before she could go to the computing lab. It had things on it like "I agree that I will not engage in copyright infringement". I asked her if she understood what copyright infringement was or what activities would constitute that. She had no idea. There are plenty of adults who have absolutely no idea. Had anyone at the school talked to her about it? No.

There is just not a lot of dialogue. I think the role of government in those contexts, perhaps, as has been mentioned already, is to facilitate education, to provide more opportunities to community groups and other organizations to carry out these functions. There is a richness of opportunity, but I think there is also a paucity of information and education.

[*Translation*]

The Chair: Thank you.

As we have to discuss committee business a little later, I am going to give Mr. Angus and Ms. Davidson two and a half minutes each. If you ask shorter questions, we can get through this.

Mr. Angus, you have two and a half minutes.

[*English*]

Mr. Charlie Angus: Thank you.

It's been a fascinating discussion. I certainly think we always have to keep the potential in mind. Indeed, the democratic involvement of new media is very transformative.

My concern is about the issue of function creep, this notion we're hearing around the table that if you sign an agreement, you make your consent. But you consent for a specific piece of information that you share, and yet that information is then re-shared and re-shared into this vast data mine. This is a question of privacy rights that has to be clarified when we are signing onto something.

My daughter in grade 9 emailed me the other day and told me she wasn't allowed on her Gmail account unless she gave Google her cellphone number. I thought that was really odd. I phoned her and asked her what happened. She told me she couldn't get her Gmail unless she gave Google her cell number.

The next day my Gmail account came up, and it told me to put in my cellphone number, please, for greater security. I didn't want to give them my cellphone number. My grade 9 daughter is smarter than me, and she wasn't going to give hers. You had to look down at the bottom of the page for a very small thing that said "Click if you don't want to do this".

When you look at it, they were asking my 14-year-old daughter to give them her cell number. Now, Google is a great corporate citizen, but she didn't sign on to Gmail to give them her cellphone information.

I guess in this question of function creep, I'm wondering what role we have in terms of saying, okay, wait a minute; that's beyond the pale. Are you going to use this cellphone number of a teenaged girl strictly for her personal security, or is this going to be added into the vast data mine that someone else is going to be able to access?

I think these are questions that we have an obligation to ask as legislators.

Dr. Valerie Steeves: Perhaps I can make just one quick comment.

If you look at identity theft, typically the solution is always "Give me more of your information so I can make sure it's you", which just creates more leaks, which just increases the risk that the information will flow and be used against you.

So to call it a "security" measure is kind of funny.

Dr. Teresa Scassa: To go back to a point that was made earlier, the notion of transparency is an incredibly important one, because people aren't necessarily aware that the piece of data that they give consent to in one context—or that they've given a certain consent to but may not have realized the scope of that consent.... They may not realize the nature of the bargain between themselves and the free company. A lot of people don't realize that Gmail is scanned to extract personal information and that this is part of the bargain with Gmail. So there's a lack of transparency at that end.

There's also a lack of transparency at the other end, when you go on a website. Professor Steeves has described a number of contexts where you're presented with advertisements when you go to read the paper, go to MSN, or wherever. I think there's a lack of transparency. People don't necessarily realize that what they're seeing is different from what other people see, and that there is a reason for that.

I don't know if that's partly a norm setting. We've also talked about setting boundaries, not just letting everything be carried by the consent model, but actually setting some norms or boundaries, which I think is a positive thing.

Then there's the increasing transparency dimension of the problem and whether that's greater public awareness or obligation on companies to do more to be more transparent.

● (1235)

[*Translation*]

The Chair: Mr. Geist has 30 seconds for a quick answer.

[*English*]

Dr. Michael Geist: I'd just note that there are companies that address the issue that we've been hearing about, this notion that they think you're someone, but perhaps you're not that person. For example, even Google gives you that ability, and it's quite striking when you do it. Google has a section where they'll tell you who they think you are and what you like based on all the information they've been able to cull.

Now, you can have them turn that off if you want. You can also tell them they have it wrong, and that this is actually who you are, because you want to see stuff that better reflects some of your interests. Some people say they don't want to tell them who they are or what their interests are. Other people say they'd rather see that sort of stuff.

My point is that there are companies out there that are thinking about those issues. If we can get the right framework with the right incentives from a regulation perspective, I think there are some good opportunities here.

[*Translation*]

The Chair: Thank you.

We will wrap this up with Ms. Davidson. You have about two and a half minutes.

[*English*]

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

My question is going to be for Professor Steeves.

I was certainly very interested in the research you've done on children's privacy. I have two or three questions. I'll ask them and then let you address them if you can.

First of all, do we have access to this study? What ages were the children that you did the research on? How did you define "personal" or "private" information when you were talking to these kids?

We've had a very high incidence of suicide with young people in my riding. I just spoke with a very concerned, distraught parent this week whose daughter was 14 years old and had threatened suicide. She had not committed suicide, thank goodness, but it came down to where the parent was thoroughly convinced that it was social media that had tipped the balance and caused the worst threat to this child. It was over a release of information that was going broadly across the community in the school of things that she felt were personal.

Could you comment on those questions, please?

Dr. Valerie Steeves: The study was conducted with children between the ages of 11 and 17, and parents with kids of those ages. It's available online, and I'd be happy to make it available to the committee. We also collected a lot of data about cyber-bullying, which is what you're alluding to, the problem that people can say things in this environment and kids can take it the wrong way and lose control.

Our data actually suggest the opposite. The kids we talked to indicated that cyber-bullying was easier to deal with than real-world bullying because it leaves a paper trail. You can point and say, "See, she said that", and you can go to adults and get some help. They were well aware of the fact that kids are more likely to say things that are a little bit more outrageous because it's not face to face. But they said, "Well, that's easy, as you can just confront them face to face; and if not, then you go and get a parent. That's when you need help from your parents".

There isn't a lot of empirical evidence to support the position that this form of bullying is actually exacerbating suicidal tendencies. There is evidence to suggest it's the opposite, that it's actually easier to deal with.

What we did get very clearly from the kids, and you'll see that if you look at the report, is that their schools' response to bullying has been with zero-tolerance policies and total surveillance. That means they can't go to the school, they can't go to the teacher, even if it's a teacher they trust, because they know the principal will be called in, then the cops will be called in, and they'll lose control.

In many ways, we're over-reacting to a particular problem and not giving them the support they need precisely because we're trying to protect them.

[*Translation*]

The Chair: Thank you.

That concludes the testimony. I thank you for being here today and I hope that we can meet again. I feel sure that your testimony will help the members of the committee in their deliberations.

We are going to suspend the meeting for a few minutes.

Before we finish, Ms. Steeves, for those documents that you are going to send to the committee, all you have to do is send the link or the documents to the clerk.

● (1240)

[*English*]

Dr. Valerie Steeves: Yes.

[*Translation*]

The Chair: We will make sure that all committee members get access to them as quickly as possible.

With that, we suspend the meeting for a few minutes and then we will move to committee business.

● (1240)

(Pause)

● (1240)

The Chair: We now resume the meeting.

Before we start, I should tell members of the committee that the information commissioner has sent in her "report cards" as we call them here. For your information, if you want to see them, they are available.

Mr. Del Mastro, do you want to speak before we begin?

[*English*]

Mr. Dean Del Mastro: As we're now in committee business, Mr. Chair, I would move that the committee go in camera.

[*Translation*]

The Chair: Unfortunately, we cannot debate that motion.

Mr. Alexandre Boulerice: I ask for a recorded vote.

The Chair: That being the case, I will let the clerk conduct the vote.

(Motion agreed to: yeas 6; nays 4. [*See Minutes of Proceedings*])

[*Proceedings continue in camera*

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

SPEAKER'S PERMISSION

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

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

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

PERMISSION DU PRÉSIDENT

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

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