HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

# Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 046 • 1st SESSION • 41st PARLIAMENT

**EVIDENCE**

## Tuesday, June 19, 2012

## Chair

**Mr. Pierre-Luc Dusseault**

# Standing Committee on Access to Information, Privacy and Ethics

**Tuesday, June 19, 2012**

● (1100)

[*Translation*]

**The Chair (Mr. Pierre-Luc Dusseault (Sherbrooke, NDP)):** It is 11:00 a.m., so let's start the meeting right away.

My thanks to Mr. Kardash, from Heenan Blaikie, and Ms. Grimes, from the University of Toronto, for being with us today. We are waiting for two other witnesses who were supposed to be here at 11:00 a.m. Our information is that they are on their way.

We will start with the presentations, for which you each have 10 minutes. Then there will be a question and answer period.

So let's start right away with Ms. Grimes.

[*English*]

**Dr. Sara Grimes (Assistant Professor, Faculty of Information, University of Toronto):** Thank you for this opportunity to speak with you today.

Over the past several years my research has focused on some of the social media sites most popular among children, from online communities like Neopets to virtual worlds like Club Penguin. These types of sites don't look very much like Facebook, but they nonetheless do allow for many of the same types of social interactions and activities we identify as characteristic of social media.

Privacy issues are of enormous relevance within these environments. The research shows that since the very early days of the World Wide Web, kids' privacy rights have been infringed upon for commercial purposes within certain online social forums. This happens with much greater frequency than most of the other risks associated with kids online. It's also something that in other countries has led directly to the establishment of child-specific privacy legislation. The key example here is the U.S. Children's Online Privacy Protection Act, or COPPA, which was initially created in response to the then growing practice of soliciting names and addresses from children in order to direct-market to them.

Today the type of data collected from kids and the purposes for which it's used have both expanded significantly. The article that was circulated to you in advance of my appearance here today describes this shift in detail, explaining industry trends toward data mining, in which children's conversations, behaviours, and ideas can become fodder for market research and product development.

In my work in this area, I have observed that within social media forums, when children are considered at all, concern for their rights often plays second fiddle to narrowly defined notions of risk. Children are still very much more often seen as potential victims or conversely as potential criminals in the online environment. As such, the emphasis is placed on protecting them from strangers, from each other, and from themselves, rather than supporting and empowering them as citizens.

This tendency has greatly impacted the way in which social media companies address child users. The first and most common response has been to simply ban children under the age of 13 from participating in social media sites. This was the strategy found until very recently on Facebook, and it remains common throughout other popular social media as well. Although some children may, and often do, bypass these bans—by lying about their age, for instance—a formalized age restriction still has deep impacts on how and where children use social media. It also serves as a way of deflecting some of the public and regulatory scrutiny that can be associated with sites that do openly allow children or invite children to participate.

While in some cases age restrictions may very well be appropriate —there are many sites where they would be—in others, the no-children-allowed approach has more to do with wanting to avoid the risks and complications that kids might bring than it does with the actual content or activities that unfold there, which means that younger children are frequently banned from participating fully and inclusively in online culture and from reaping many of the benefits and opportunities that social media presents, simply because it's been deemed too much work or too expensive or simply too risky to accommodate them.

Another increasingly common response is the creation of tightly controlled child-specific social media, found in social networking sites, virtual worlds, and online communities designed and targeted specifically to children, usually under the age of 13. In my research I've found that in many of these cases the emphasis on risk has put privacy front and centre. Privacy concerns integrated at the level of design are quite apparent. They surface in legal documents such as privacy policies in terms of use, and they appear in the marketing of the sites themselves.

However, a number of areas are in dire need of improvement. As mentioned, there is continued evidence that children's online interactions are being surveilled and data-mined, most often without the full knowledge or consent of the kids involved, or that of their parents and guardians. While kids are regularly asked to agree to these kinds of activities through the privacy policies and terms of use they are required to agree to in order to participate, even on sites designed and targeted to younger children, these documents are long and extremely complex. They describe a wide variety of data collection activities and include a number of terms that are inappropriate and even inapplicable to ask children to agree to.

This raises important questions about informed consent, an issue that's particularly pressing when the users consist of young children with widely varying literacy levels and emerging capacities for understanding complex legal relationships. Best practices would include providing a child-friendly version of both of these documents to ensure that children and their parents know exactly what they're agreeing to. While there are definitely some really great examples of this practice out there, overall very few sites for kids bother to do it. When they do, the child-friendly versions are rarely comprehensive: most don't explain the full reasons for user data collection or only describe items that present the social media company in a positive light.

● (1105)

The misrepresentation of children's privacy as a matter of online safety is also becoming an increasingly prevalent trend. Now, don't get me wrong here. A broader consideration of how rules and design features aimed at protecting children's privacy rights might also offer protection from online predators and bullies has some very real benefits for children's safety and for their enjoyment of social media. But so far, in many cases this dual function has been realized in ways that work primarily to obscure the underlying commercial practices that privacy policies are actually meant to address. By reframing children's privacy as predominantly a matter of online safety—which is, in these cases, defined as safe from other users—the more mundane and less obviously risky threats to children's privacy, such as corporate surveillance and invasive market research, are sidelined.

A related emerging trend is to commercialize the safety features themselves, as I discovered in a recent study of kids' virtual worlds. Some kids' virtual worlds come with a “safe chat” version, where chat between users is limited to selecting preconstructed sentences from a drop-down menu. In one case, the “safe chat” version limited kids' options to a mere 323 different phrases, 45 of which were cross-promotional and 30 of which promoted third-party ads. As you might have guessed, none of these phrases were in the least bit negative. Kids could chat about how much they loved the brand but were prohibited, by design, from saying anything critical about it.

Among the many potentially negative impacts this can have on children is the impact it has on children's rights. These examples reveal that an unfortunate trade-off is taking place, as limited approaches to children's privacy and safety can place undue restrictions on children's other rights, such as the right to freedom of expression or the right to participate freely in cultural life.

Now, it's important to note that what I've described here are general trends, mostly found in commercial social media sites that are considered to be popular among children. Not all social media companies follow these practices. And there are, in fact, a number of Canadian companies that have come up with some pretty brilliant alternative strategies for balancing kids' privacy, safety, self-expression, and cultural participation. There is potential for real leadership here, but there's currently a lack of the kind of regulatory and government support that would be necessary for these types of individual, small-scale, ethical, rights-based approaches to develop into widespread industry practice.

In the time I have left, I'd like to outline four key take-aways or recommendations.

First, there is a clear and growing need for child-specific regulation on the collection, management, and use of children's data. In so doing, however, we'll need to avoid making the same mistakes that have plagued certain previous attempts, such as COPPA, in the U.S., which resulted in kids losing access to certain very important social spaces and/or widespread lying about their ages. We'll also need to expand this regulation in ways that better reflect current and emerging online data collection practices.

Second, we need a much clearer articulation of the ethics of informed consent where children of various ages are involved.

Third, we need to strive for a better balance between children's privacy rights and other rights, such as freedom of expression and the right to participate in cultural life, both within our discussions of these issues and within regulations, either amended or new.

Last, we need to establish clearer leadership and stronger enforcement of these child-specific rules, which would include acknowledging and supporting the innovative, ethical, rights-based examples that certain independent and small Canadian social media companies are already working to build.

I look forward to discussing these issues further with you during the question period.

Thank you.

● (1110)

[*Translation*]

**The Chair:** Thank you very much.

I now give the floor to Mr. Israel.

You have 10 minutes.

[*English*]

**Mr. Tamir Israel (Staff Lawyer, Canadian Internet Policy and Public Interest Clinic):** Good morning.

My name is Tamir Israel, and I am a staff lawyer with the Samuelson-Glushco Canadian Internet Policy and Public Interest Clinic, CIPPIC for short. CIPPIC is grateful for this opportunity to present its views on the privacy implications of social media to the committee.

CIPPIC is a legal clinic based at the University of Ottawa Centre for Law, Technology and Society. We advocate in the public interest on issues arising at the intersection of law and technology.

Since its inception, CIPPIC has taken an active part in legal and policy debates about online privacy, both domestically and internationally. Our clinic filed a complaint that led to the first comprehensive investigation of international social networks' privacy practices.

[*Translation*]

**The Chair:** Just a moment, Mr. Israel. Could you read a little more slowly, please, so that the interpreters can do their job properly?

[*English*]

**Mr. Tamir Israel:** I'll talk a little slower.

The growing importance and benefits of social media to Canadians cannot be understated. These are far-reaching and permeate every aspect of our individual, social, and political lives. The innovative and commercial growth of such networks should not be unduly restricted. At the same time, Canadians should not be forced to choose between their privacy rights and their right to participate in this new interactive world.

PIPEDA, which forms the backbone of privacy regulation in Canada, provides a flexible set of principles that cater to the legitimate needs of businesses while providing safeguards for user privacy. While PIPEDA has largely withstood the test of time, the privacy landscape has changed substantially since its enactment, and a decade of experience has exposed a number of shortcomings that should be addressed if the statute is to continue to meet its objectives.

I will quickly say a few words about the shifting privacy landscape and proceed to elaborate on four areas that I think need immediate attention.

In recent testimony before this committee, Professor Valerie Steeves pointed to research indicating growing lack of trust in online companies. A survey conducted for Natural Resources Canada in late 2009 similarly found that respondents' level of trust in different types of organizations to keep their personal information secure is moderate to low. The least trusted were small private sector businesses and social networking sites.

The study similarly found that the ability to control the context in which information is shared increased levels of trust. In another study conducted by researchers at Annenberg and Berkeley, 67% of Americans agreed or strongly agreed that users have lost all control over how personal information is collected and used by companies.

Feeding this sense of lost control is an increasingly complex ecosystem where the scope and nature of data collected increases daily, even as the sophistication of information collection and analysis mechanisms keeps pace. While Google and Facebook have been at the forefront of debates on these issues, numerous other companies are involved. Acxiom, a data broker based in Arkansas, has reportedly collected an average of 1,500 data points on each of its 500 million active user profiles.

Few of these users have heard of Acxiom, let alone had any direct interaction with the company. Yet the profiles, which data brokers such as Acxiom sell, are populated with their browsing habits; the Facebook discussions they have with their friends and family; their sensitive medical and financial information; their ethnic, religious, and political alignments; and even real-world locations visited. All this data is collected, analyzed, and refined into a sophisticated socio-economic categorization scheme, which Acxiom's customers use as the basis of decision-making.

The sheer complexity of the ecosystem that fuels databases such as Acxiom's defies any attempt to articulate within the confines of a privacy policy. A number of jurisdictions are looking at ways of addressing the need for greater transparency and choice. I will briefly focus on four here that I think are relevant specifically to PIPEDA. I'll point out as well that the nature of the data being collected in this ecosystem is also increasing in sensitivity. Newly emerging capacities are aiming to incorporate real-time location and even emotional state into the categories of information that are available for targeting. I'll touch on four changes I think we should focus on. The first is transparency.

Greater transparency is needed. To this end, the United States Federal Trade Commission has recently stated it will push data brokers to provide centralized online mechanisms that will help users discover which data brokers have collected their data. This can serve as the basis for the exercise of other user rights.

Informing users can be achieved in a number of contexts through greater integration of notification into the service itself. This not only allows for greater flexibility and nuance in notification, but also increases privacy salience by reminding users in context of the privacy decisions they are making. In addition, elements of privacy policies can be standardized, but care must be taken not to oversimplify data practices that are in reality complex. The dangers of oversimplification are that organizations will begin to rely on blanket and categorical consent, which are simple but do not provide customers or advocacy groups the details they need to properly assess their practices.

● (1115)

Another area I'd like to touch on is privacy by default or privacy by effort, which is an analog to that.

Transparency alone is not enough to protect privacy in this interconnected age we are in. In a recent consultation process on online privacy, it was noted that many online services are public by default and privacy by effort. New users will rarely know how to configure the complex web of the often conflicting privacy control services that are offered when first signing on. Settings constantly shift and change, as new ones are introduced and old ones replaced, or when new features are added to existing services. Simply maintaining a constant level of privacy is a never-ending effort.

Compounding such efforts is a tendency for social networking sites to make occasional tectonic shifts in the constitution and nature of their services. These are often imposed on ingrained users as “take it or leave it” propositions. At other times, pre-selected defaults are used to nudge users in directions that are very different from the service they have grown accustomed to.

As you've heard from other experts, the devil is indeed in the defaults. Stronger protections are needed to ensure new services and settings are introduced with privacy-friendly defaults that reflect the expectations of users and the sensitivity of the data in question, not whatever configuration is best fitted to the service provider's business model.

Under PIPEDA, the form of consent should already be tailored to user expectations and the sensitivity of the data that might be affected. However, in order to firmly ingrain this concept in service design, privacy by default should be explicitly adopted as a principle under PIPEDA.

Another area I want to touch on briefly is enforcement and process.

The committee has heard from a number of parties about the importance of ensuring that the Office of the Privacy Commissioner can enforce its powers. Adding bite to PIPEDA is critical for a number of reasons. First, it is necessary in order to provide incentives for compliance. Currently there are very few penalties for non-compliance. In most cases the most an organization can expect is the threat of being publicly shamed for non-compliance. Second, having these powers in place will assist the Office of the Privacy Commissioner in its interactions with large multinational organizations so it can carry out its mandate in protecting the privacy of Canadians.

In addition to adding penalties, procedural changes to the OPC's investigative and compliance framework should be explored. Compliance with OPC recommendations in a social networking context may be a long and complicated road, requiring changes to system design. However, under PIPEDA the OPC's legal mandate to exercise its powers over a particular complaint ends 45 days following the issuance of an official finding. The mechanism lacks the flexibility necessary to ensure Privacy Commissioner recommendations are carried out adequately.

Finally, I'll touch briefly on breach notification requirements.

Canada is in dire need of a breach notification obligation. Such an obligation will improve incentives to build stronger technical safeguards and provide users with opportunities to redress harm, such as identity theft and the potential humiliation that may result from a breach of their data.

Bill C-12, which is currently in first reading, provides a workable framework for breach notification, but it requires fixes and a commitment to introduce penalties for non-compliance if it is to be effective.

I would be happy to elaborate further on any of these points. CIPPIC plans to file a more detailed brief with the committee at a later point.

Thank you very much for your time and attention.

● (1120)

[*Translation*]

**The Chair:** Thank you for providing us with your presentation.

We now move to Mr. Kardash, also for 10 minutes.

[*English*]

**Mr. Adam Kardash (Managing Director and Head of AccessPrivacy, Heenan Blaikie):** Good morning, Mr. Chair and honourable members. Thank you for the opportunity to speak with you today.

My name is Adam Kardash. I am a partner at the national law firm of Heenan Blaikie, and chair of the firm's national privacy and information management practice. I am also managing director and head of AccessPrivacy, a Heenan Blaikie consulting and information service focusing on privacy and information-related matters.

I appear before this committee in a personal capacity, representing only my own views. However, my views are based upon my experience at Heenan Blaikie and AccessPrivacy.

Over the past ten years I have focused almost exclusively on advising private sector organizations on privacy and information management matters. I regularly consider the privacy law implications of new technologies and platforms.

In my opening remarks I will offer a number of comments that centre on a single theme; namely, that our federal private sector privacy law, the Personal Information Protection and Electronic Documents Act, or PIPEDA, works very well. Since coming into force in 2001, and despite all sorts of criticism from a range of stakeholders across the Canadian privacy arena when first introduced, the statute has stood the test of time. In my view, PIPEDA has worked and continues to work particularly well in addressing privacy challenges raised by new technologies.

The act sets out a comprehensive set of requirements that regulates an organization's collection, use, disclosure, storage, and management of personal information. One of the reasons the statute remains effective today is because it was drafted in a technologically neutral fashion. PIPEDA's core rules are mainly set out in plain language as broad principles, and therefore can be applied to any new technology, new application, or new system that involves the processing of personal information, including social media platforms.

It is precisely because PIPEDA does not focus on any particular type of technology that it is so well suited to addressing seemingly novel privacy issues that may be raised by new technological developments. In this regard, it is important that PIPEDA remains drafted in a technologically neutral manner. Given the increasingly rapid pace of technological innovation, any statute that is drafted focusing on a certain technology or platform, whether social media or otherwise, will be obsolete, out of date, by the time it comes into force.

In my experience, technology-based issues, privacy or otherwise, are most effectively addressed through self-regulatory frameworks that work in concert with the statutory regime. Compared to statutes or regulations, self-regulatory frameworks are far easier to develop, implement, supplement, or revise in order to remain current with changing technological developments.

Notably, under PIPEDA, a self-regulatory framework developed by way of a meaningful consultation process would have legal value under the statute. Self-regulatory frameworks establish industry standards, and well-developed industry standards inform the meaning of PIPEDA's overarching reasonable person test. This is in subsection 5(3) of the act, which provides that organizations may only collect, use, or disclose personal information for a purpose that a reasonable person would consider appropriate in the circumstances.

When advising clients, as a matter of practice I do not refer to PIPEDA as merely a set of legal rules. Rather, the statute sets out a useful framework for organizations to proactively address privacy concerns in a manner that balances individual privacy with the collection, use, and disclosure of personal information in the course of legitimate business activities. PIPEDA's rules are dynamic, in that they apply to the entire life cycle of data, from the collection or creation to the ultimate destruction of personal information held by an organization.

All of these rules fall under the principal feature of PIPEDA: the accountability principle. The accountability principle is a simply worded but very powerful requirement. It provides that organizations are responsible for personal information in their possession or control.

Notably, PIPEDA's accountability model is now being referred to around the world, by foreign data protection authorities, foreign governmental bodies, and global privacy think tanks, as the enlightened statutory model for the protection of personal information. PIPEDA's framework, in large part due to its accountability model, is specifically cited in these international fora as being well positioned to appropriately address the privacy concerns that may arise in the online sector, and otherwise in the technological context.

● (1125)

There are a number of published letters of findings from the Office of the Privacy Commissioner of Canada that clearly demonstrate the OPC's effectiveness, under PIPEDA's existing framework, in considering and appropriately resolving emerging privacy issues raised by new technologies. They include several letters of findings issued in the social media context.

One of the central and in my view critical features of PIPEDA is the ombudsman model incorporated into the act. The Privacy Commissioner is vested with the role of ombudsman in carrying out her duty to oversee the personal information practices of organizations subject to PIPEDA, with recourse to the Federal Court where issues remain unresolved.

The ombudsman model is hardly new. It is typically employed by governments to regulate public administration. But PIPEDA applies the ombudsman model, in a novel fashion, as a means of regulating private sector activity. In my experience dealing and interacting with the OPC when advising clients across all sectors, the OPC's ombudsman model has proven over time to be very effective and generally well received by private sector organizations.

An ombudsman model is particularly well suited to facilitating effective privacy compliance, since meaningful privacy protection is not just about an organization satisfying legal rules. Rather, privacy interests are addressed meaningfully when a privacy mindset is fostered within an organization in a manner that's tailored to the reality of an organization's business context. Experienced chief privacy officers understand that privacy is about enhancing trust. And building trust requires engaged discussion with stakeholders within an organization, within industry sectors, and across the privacy arena. The OPC plays an important part in this discussion, and the ombudsman model facilitates flexible and collaborative interaction with private sector organizations.

Commissioner Jennifer Stoddart eloquently described the nature of her role as ombudsman in a 2005 speech in which she considered the merits of the ombudsman model. She stated:

> It must be underscored that the Ombuds-role is not simply remedial, but transformative in nature. The aim is the resolution of individual complaints, but it is also the development of a lasting culture of privacy sensitivity among parties through their willing and active involvement in the process itself. In order to achieve these twin goals, the process must necessarily be flexible, participative and individuated in its approach.

Recently there have been calls from various stakeholders in the Canadian privacy arena, including from Commissioner Stoddart, for PIPEDA to be amended to provide the OPC with greater enforcement powers. Based on my experience in the privacy arena over the last ten years, it is not clear that any such amendments are necessary.

To their credit, Commissioner Stoddart and the more recently appointed assistant commissioner, Chantal Bernier, have been remarkably successful in carrying out their mandate in the ombudsman model context. They have done so with an arsenal of several powers under PIPEDA. In particular, they have the power to publicly name organizations that are in breach of PIPEDA, the power to self-initiate investigations or audits of an organization's personal information practices, and, as I noted, the power to refer complaints to the Federal Court.

The OPC has been highly respected in the international privacy arena for years, but it enhanced its reputation considerably among foreign data protection authorities as a result of its highly publicized investigation of Facebook's personal information practices. As a direct result of the OPC's enforcement activities, Canada is now regarded as one of the leading jurisdictions globally, exploring privacy issues associated with new technologies, including in the social media context. The OPC's achievements in this regard have been accomplished without order-making power or other enforcement mechanisms, such as the ability to levy fines. Notably, Commissioner Stoddart has made public statements to the effect that the mere public threat by the OPC of potential Federal Court action against a given organization has almost always resulted in the organization satisfying the OPC's concerns.

Innovative new technologies, such as social media platforms, offer Canadians tremendous value. As we continue to engage with and take advantage of new technologies, and we all provide our personal information in the course of doing so, privacy will continue to play an increasingly integral part of private sector organizations' trust relationship with individuals.

As we consider emerging privacy issues, it is of course important to reflect upon whether the existing privacy regulatory framework serves to ensure that individual privacy is appropriately addressed. With PIPEDA, we're fortunate: we have a technologically neutral, principle-based statutory framework that has served us exceedingly well in ensuring the protection of privacy in a balanced fashion.

● (1130)

As the committee continues its study, I respectfully offer the following concluding suggestions when it considers whether and the extent to which PIPEDA needs to be amended to address challenges posed by new technologies, in particular, amendments that will provide enhanced enforcement powers.

First, as individuals we all have a responsibility to be careful with how we use our personal information in public contexts. Public outreach and regular training and awareness by privacy regulatory authorities and relevant private sector organizations are critical in this regard. No amendments to PIPEDA would be required to enhance our collective efforts in this fashion.

Second, I respectfully submit that the committee carefully consider the costs of moving to an enforcement model under PIPEDA. To accommodate new enforcement powers such as order-making power, structural changes to the OPC will be required, and key benefits afforded by the ombudsman model will be lost.

Third, as part of a national strategy to ensure growth of our domestic technology sector, we need to ensure that any legislative change or initiative be carefully considered in a manner that ensures we don't impose unnecessary impediments to legitimate business activity. In short, in my view, the economic costs of privacy regulatory change need to be carefully considered. We need a regulatory framework that fosters innovation. In the privacy arena, PIPEDA provides us now with an appropriate model that has served us well in this regard.

Finally, the constitutional impact of any legislative change to PIPEDA, in particular with respect to new enforcement powers, needs to be carefully reflected upon. The recent Supreme Court of Canada decision in the securities reference, a case that considered the constitutionality of a national securities administrator, serves as an important reminder that constitutional considerations need to be a part of any study of privacy legislative reform.

Thank you again for the opportunity to speak with you this morning. I would be pleased to respond to any questions from the committee.

[*Translation*]

**The Chair:** Thank you.

Now it's time for questions and comments.

Mr. Angus, you have seven minutes.

[*English*]

**Mr. Charlie Angus (Timmins—James Bay, NDP):** This is another fascinating day of discussion.

I would like to start with you, Madam Grimes, because I think what you're suggesting seems to be somewhat counterintuitive to the message we've been given, which is that we have to limit young people on social media, that we need to have these limits for 13-year-olds. I don't know any kid under 13 who isn't on Facebook or on social media. They're not allowed to do it at school. They're not allowed to go to YouTube at school. So they're supposed to be staying off social media, but we'll create these little walled gardens for them to protect them.

These walled gardens are run by corporate interests that you're telling us mine their data and sell their data and basically are using this as a bit of a commercial predatory space. Would it be better that we establish some clear rules to limit companies' ability to go after this kind of right, the privacy of information of children? Should we actually move young people onto general social media with some better rules? Would that be a better solution than these walled gardens that are being set up now?

**Dr. Sara Grimes:** Yes, I definitely think so. Yes, in pointing out the two trends, both models have resulted in some pretty clear infringements of kids' rights and some huge problems. Banning kids from Facebook hasn't kept kids off Facebook, as you've said, and creating the walled gardens has created this false sense of security and safety for parents and for children who are seeking those types of alternatives, where a lot of other processes are going on unchecked.

Again, it's not that every social media site that's designed specifically for kids is doing this to the same extent, but it is this trend that has been spreading and kind of deepening as time goes on. So yes, I in no way meant to suggest that banning kids or creating walled gardens was the ideal, but these are the things that have happened over the past ten years.

This is the state of affairs: neither model works. So now I definitely think that we need to start looking at alternatives, at the possibility of creating a better framework that would give different social media companies a guideline and baseline to work from that's not based purely on reacting to public outcries about risk and parental concerns about risk, but on something broader, on a more democratic sort of sensibility about rights in general. It would weigh all the different benefits that kids can get from participating in social media, along with the risks. I think a lot of companies would really benefit a lot from having those kinds of guidelines and frameworks in place.

● (1135)

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

Mr. Kardash, I'm hearing two very different views, one from Mr. Israel and one from you. He says we need breach notification, we need compliance orders, administrative monetary penalties. You tell us that the market works best when it's left to do what it wants to do, and Commissioner Stoddart is perfectly happy with the state of affairs.

You don't believe there should be better compliance rules?

**Mr. Adam Kardash:** As I mentioned in my remarks, PIPEDA currently establishes, in my view, a very effective model for the protection of privacy in a manner that balances the interests of both individuals and businesses in the course of their collection and use of data in the course of legitimate business activities.

There currently is a series of powers that the commissioner does have, which, by the evidence of over the last several years, have been remarkably successful—to their credit—in addressing these very issues.

**Mr. Charlie Angus:** What powers? She said her powers aren't sufficient.

**Mr. Adam Kardash:** In my view, the current model and powers are entirely sufficient.

**Mr. Charlie Angus:** Okay.

I just have a question. You didn't tell us you were Facebook's lawyer. Or did I not hear that? Did you tell us you were Facebook's lawyer when you came here?

**Mr. Adam Kardash:** I act for a range of companies in the social media space. They are one company. I am here purely in my personal capacity.

**Mr. Charlie Angus:** Okay.

So Mr. Israel writes you a letter, Mr. Kardash, on May 28, 2010. He says to you, with respect to your client's compliance with PIPEDA, your client being Facebook, that

> ...we wish to note that the privacy screen it intends to present its users is not...an adequate basis for curing the concerns we raised with your client in respect to its December privacy transition. Our position is that Facebook does not have the meaningful informed consent of its users for privacy changes....PIPEDA requires both transparency and privacy sensitive defaults in line with user expectations.

You were there representing Facebook in one famous case of compliance. We still don't seem to have really worked out compliance, from what we're hearing from the Privacy Commissioner.

Don't you think you should have told us that's who you represent?

**Mr. Adam Kardash:** The Office of the Privacy Commissioner of Canada has considered multiple investigations in the social media context, including several involving Facebook. All of them have been resolved to the satisfaction of the Office of the Privacy Commissioner of Canada. They've considered those carefully.

Again, I'm here not on behalf of any one particular company; I'm here on behalf of a range of companies and views.

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

Mr. Israel.... And again, I'm not picking on Facebook here. I love Facebook. I'm on it much too much, according to my wife especially. She thinks I have a Facebook addiction. I should go on the record with that. I might have a problem.

Mr. Israel, you mentioned Acxiom. You see, we're focused on Facebook, we're focused on Google and whether they're in compliance or not in compliance. But in the age of big data, there are third-party data-miners who are out there well beyond the scope of anything we're even aware of. You mentioned this company Acxiom. You said they have 500 million hits. We've never even heard of it.

How do we ensure some measure of compliance with the data-miners who are going in, and through their...? It's fairly easy just to gather up massive amounts of information. It's not like we want to pick on Facebook or pick on Google; there are companies that are gathering this information and we have no idea of them. What steps do we need in order to deal with these companies?

● (1140)

**Mr. Tamir Israel:** Well, it's definitely a challenging arena. I agree with Adam to the extent that we should be putting in place flexible regimes that don't shut down legitimate innovation and these types of things. I'm also on Facebook, and I like the services.

I think there's a gap between the user understanding and expectation of what's happening when they interact with their friends and their colleagues in some of these online venues and how the information flow works. A lot of the interactions happen in a semi-public context in social media, and companies like Acxiom are free to basically suck that up into their databases. This is probably a violation of Facebook's terms of use, but there's no transparency in this process. Nobody really follows very closely how the information is getting into these databases or what the rules of collection are.

With respect to the database data brokers in particular, it's a challenging environment. There's no direct interaction with the users, so you need.... The FTC is looking at putting in place some rules that will stimulate industry to provide centralized places where users can go and check which data broker has a profile on them, what they have, and where it came from.

That may be one starting point for it. We don't need heavy-handed fines or anything like that in this context, but at least the threat of a penalty, if you continually ignore the principles that are there, is very necessary to get both proactive and reactive compliance. I'm not saying everybody's a bad actor, but without the possibility of a penalty, there's often little incentive to practicably figure out what these principles are and really integrate them into your business model.

**Mr. Charlie Angus:** My concern is—

[*Translation*]

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

[*English*]

**Mr. Charlie Angus:** I was just getting started, Mr. Chair.

[*Translation*]

**The Chair:** You are almost at nine minutes.

I now give the floor to Mr. Calkins, for seven minutes.

[*English*]

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

Thank you very much to our witnesses. We've heard some fascinating information here.

I don't even know where to begin, but I'm going to just start, Ms. Grimes, with you.

You said that unbeknownst to most Canadians—I think this is fairly common knowledge—online activities are surveilled. We have data-mining going on out there. We have spiders. We have bots. We have all kinds of things that are downloaded onto people's computers unwittingly. We have spyware, malware, adware, and whatever you want to call it tracking people's activities, whether they're on a laptop or a mobile device. In these user agreements, we agree that our information will be allowed. It's in our settings in our devices whether or not we want to allow cookies, for example, on our computers. It's in our settings on our iPods and our iPads. We get push notifications. We can turn these kinds of things on or off. An educated user will have to make a little bit of an effort to do that. We can get third-party software that will help us protect, for example, our computers at home that our children are on when they're trying to do their homework, so that I as a parent can get notification on what kinds of activities my children may or may not be doing online.

And that's going to be a question I have for you: Do you think my child has the right to be able to do that on a computer, without me knowing what my child is actually doing? I'll save that question for the end.

In all of these agreements, I have one choice: I either accept the terms of the agreement in its entirety or I don't. That's the choice I have. I don't have the option to parse parts out.

My question, broadly, for all three of you is do you think there should be a legislative or a regulatory requirement to have these kinds of agreements parsed out in such a way that an end-user can actually have the ability to select which parts they're going to agree to, or which parts they're not going to agree to? Most of these things set defaults on how my information is going to be shared with a company like Acxiom, which frankly has me terrified.

I know how these things work, because I used to be a database administrator. I understand how these data points are collected, and many of these things are collected without my knowledge. I'm sure my name's in Acxiom, because I'm an avid computer user, or if it's not in Acxiom it's somewhere else. Somebody has information about me and my browsing habits and my user habits, and so on. So this is a very frustrating thing.

Why can I as a user not have the ability to choose which parts of the agreement I want to agree with and which parts I don't? Is that a reasonable thing, from a regulatory environment point of view, for a government to be involved in?

● (1145)

**Dr. Sara Grimes:** I'll leave the broader parts of the question to my co-presenters here.

In terms of kids and user agreements, there definitely need to be some changes. I've read a lot of end-user licence agreements for service directed to kids. They include all the same types of clauses that you find in any of these documents. There are all kinds of complications when kids are involved. Not only are there words that most kids can't understand, but most adults have trouble understanding them. Service contracts actually describe relationships in terms that younger kids just can't understand yet. They still have some developing to do before they can understand that level of complex things like property exchange or different economic processes that are being described in terms of service and use.

Changes to the kids' area, which is the area I'm an expert in, are defintiely needed with regard to things like the terms used in contracts so that they are understandable to kids and parents. I think as a government, as a country, we need to start thinking about how we're going to deal with kids entering into contracts, because minors' contracts are very tricky legally. They're voidable and there are all kinds of strange precedents to wade into.

I'm not a legal expert, and it hurts my head even to think about how complicated this all becomes when you start thinking about it in those terms. But we need to start dealing with that. We need to start thinking about it seriously and think about what we are expecting kids to be held to when they agree to terms of service that are 15 pages long, are full of all kinds of jargon, and include processes that are so far beyond what they're capable of understanding that we couldn't possibly expect these contracts to actually be upheld.

So, yes, I would love to see a more à la carte type of design for terms of service for use and end-user licence agreements, including some terms that have been delineated as terms that are appropriate for younger kids, and a framework for figuring out how we're going to deal with who signs on and who agrees to it, and how involved will parents be, because they clearly will have to be.

**Mr. Blaine Calkins:** Thank you.

**Mr. Adam Kardash:** The question's excellent, because it illustrates how you can't address privacy in a meaningful fashion with just an upfront consent process, especially for platforms that get more complicated.

There are two approaches to dealing with all sorts of different contexts, not just in the pure technology sector, but even more broadly. One is that in addition to a meaningful drafted notice upfront about what the user should be engaged in, really the most important thing has become twofold. One part is making sure users have appropriate control, and know where they can exercise that control. The other is—and this is an absolutely critical point and the emerging theme over the practice during the last ten years—that we've seen a move from concepts of consent and notice being important parts of privacy protection to the concept of privacy governance and a much more holistic approach to how you address these issues.

I think two or three weeks ago the Office of the Privacy Commissioner of Canada and the Alberta and B.C. privacy regulatory authorities issued a joint 26-page guidance document on their expectations for effective privacy management programs. Those expectations set out obligations for organizations to look at privacy five steps back from the whole range of the life cycle of data but from a risk perspective, in a manner through which they continually improve their practices and address things like controls and transparency. But most importantly, they addressed it in a much more detailed format.

I encourage the committee to refer to that document. There are at least 110 expectations set out that really go to the heart of your question. If companies are relying solely on those long-winded consent forms.... I used to draft those things. I know what they're about. They're not effective for privacy compliance. It's privacy governance that's exactly at the heart of what you're raising.

● (1150)

**Mr. Tamir Israel:** It is an excellent question. I fully agree it is important to do a little bit more to simplify privacy policies. There's been talk of trying to standardize certain terms that have similar meanings for different companies but that are described in different ways in order to make it easier for consumers to compare privacy policies, but I agree with my colleague that doing that can't be the end of the process.

It's very important to have accountability and to have organizations put in place processes that take into account privacy concerns at all stages of the development of their services. I think our federal Privacy Commissioner and some of our provincial privacy commissioners have done a really good job at instilling that.

In addition, though, it's very important to make sure the substance of what is being imbedded into these development processes is also reflective of user expectations and privacy. Historically there's been a divide internationally among what the European Union does, what Canada does, and what the U.S. does. The U.S. had this sort of open framework where there was not too much regulation in place, but they're moving very far away from that and towards where we are now and also adopting these types of last-minute, just-in-time notifications where you're providing more notification and more control in line with the decisions you're actually making. That helps adjust elements of the privacy policy to let users have greater control over which parts of it they're okay with and which parts they're not.

[*Translation*]

**The Chair:** Thank you, Mr. Calkins.

[*English*]

**Mr. Blaine Calkins:** I have a couple of minutes left, Mr. Chair.

[*Translation*]

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

Although it is very interesting, I must now recognize Mr. Andrews, for seven minutes.

[*English*]

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

Mr. Calkins, I'm going to try to get back to your questions around parents and the role of children in this.

Sara, my question's going to be directed at you. There are kids being born today who will know nothing but Facebook. They will grow up. We're at a very critical stage of this right now as these kids are now realizing what Facebook is.

As parents we sometimes like to show our kids off, and we put them on Facebook even before they're born. Only yesterday I saw a picture of an ultrasound on Facebook.

What role do parents have in this whole debate? We start it often before they're even born. Then when they're born we put their lives out there. I guess we bear some of the responsibility here.

Is it an education thing we need to be doing here? Is there any way to stop it, or is this genie already out of the bottle and there's no moving back on it?

**Dr. Sara Grimes:** It depends what the genie includes, I guess, in terms of being public and living online. It's hard to know if that's even something we should be trying to prevent and prohibit. We're trying to figure out the best way to do it, the best way to welcome kids into this world they're being born into. There's not really an alternative. They're getting school lessons and homework that gets them on social media. A lot of social interaction happens there. There are opportunities to be political, to find out about important events. There's a ton of benefits. It's how you balance the benefits and the risks, I think, instead of just focusing on one or the other.

In terms of parents' involvement, young kids and parents often come as a unit. A lot of these things are family processes that families are going through together. How families negotiate those is really important, but it can't be left completely to the families to make these types of decisions. As you say, not all parents know everything there is to know. This is new and fast-moving. It's hard for people to keep up. It's a huge burden to expect parents to be able to monitor and regulate every single thing their kids do. If they offload that responsibility onto something like a cyber-nanny program, a number of those have actually been investigated for doing a huge amount of data-mining on the kids they're protecting from particular sites and what not.

Approaching this as a family issue is definitely a useful way to think about it, but families also need support. Families need guidelines. Families need experts and politicians and lawyers on their side as well to think about how best to manage these things and support the best practices that do emerge and not to put all the burden on individual families to come up with solutions to very complex problems.

● (1155)

**Mr. Scott Andrews:** Often people put the expectation on governments, and that has been done throughout the years. That's why we have an age for drinking. That's why we have an age for smoking. So it begs the question: Do we need an age restriction for this, and if we do, is it impossible to police, and have we already gone past that point of doing that now?

**Dr. Sara Grimes:** Comparing it to something like alcohol is a bit tricky, because there are proven health risks. There are adverse effects on development and physical development and all kinds of terrible things that can happen to young children if they're exposed to alcohol too young. I think about online space very much as being like public space. We don't have age restrictions on public spaces, on parks and the streets. Kids are allowed to be in public. If we think about being online as just an extension of being in public, then putting an age restriction on that I think is really problematic.

That doesn't mean that we can't have rules and legislation that would help guide what the practices should be and how kids should be addressed and treated. There are parts of this online public that are definitely inappropriate. I'm thinking about extreme examples here, just as in our physical world we also wouldn't let kids wander into certain stores and certain places. So I think having the same types of more nuanced, more considered rules and approaches would be applicable here, as opposed to having age restrictions. They rarely work in an online world, because age restrictions do put a lot of the onus on kids and families.

That's why I think COPPA has been deemed.... I don't think the Childrens Online Privacy Protection Act in the States is a complete failure. I think it did result in a lot of good things. Other people have deemed it a failure because kids are able to bypass the age restrictions. That's maybe taking too much of a blanket approach, and it also puts the onus on kids and parents to do all the monitoring. The age restriction is there, and if they're not abiding by it, then they're kind of punished.

**Mr. Scott Andrews:** We're dealing with minors, and there are laws about minors. How do parents like Mr. Calkins and me integrate ourselves into this? Do we have any rights to contact these companies and say "My child is on here and I need to do something, I need to monitor this"? Is that a responsibility? Is that something we as parents should be concerned about?

**Dr. Sara Grimes:** One of the actually very positive aspects of COPPA was that one section of it said parents had the right to contact companies and find out all the data that a company had collected on their child and to put in a request for the data to be destroyed. According to people who have followed up and studied how the act has functioned and not functioned over the past 10 or 12 years, apparently that was not something enacted very often. But that was one way. Presumably kids could also demand the same thing and find out what data had been collected on them and have some sort of recourse, an established solution, so that if they wanted the data to be destroyed, it could be.

**Mr. Scott Andrews:** That was COPPA, did you say?

**Dr. Sara Grimes:** Yes: the Children's Online Privacy Protection Act in the U.S.

**Mr. Scott Andrews:** Okay.

Maybe to Mr. Kardash, how does that dovetail into our PIPEDA law? Are we both there on the same page?

**Mr. Adam Kardash:** Canada doesn't have specific legislation dealing with children's privacy, but by implication.... In PIPEDA there are, among other things, consent rules. Children, and certainly children under the age of 13, would not have the legal capacity to provide their consent. By virtue of certain activities they would engage in, the consent of a parent or a guardian would be required in order for them to legally engage there. So the parent, in that vein, steps in the shoes of the child.

Probably more robust than COPPA, we have in addition to the consent rules the full range of other requirements that an organization would still have to comply with—the security, the notice to the parent, the retention practices and the destruction of personal information, and the rights of access that would be afforded to the individual parent.

So you have a full complement of legal requirements and obligations that would still suffice, but you have fundamentally that consent provision that someone under the age of 13 wouldn't have legal capacity to provide.

**Mr. Scott Andrews:** How difficult is it for—

● (1200)

[*Translation*]

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

In order to be fair, everyone must be able to speak for the same amount of time.

Ms. Davidson, you have seven minutes.

[*English*]

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

Thank you very much to each of our presenters today. This is an extremely interesting topic that we're studying here. Your input today I think raises a lot more questions and concerns that we need to address.

In particular, Ms. Grimes, you talked about some of the sites for kids and about some of the things that are available for kids. I think you said that their privacy rights can be infringed upon for commercial gain by some of these companies. You talked about other countries having safeguards. Some areas have a ban, for those who are younger than 13 years of age, with respect to whether or not they can be on these sites.

I agree, I think the consents that are required are totally inappropriate for kids. I think they're totally inappropriate for adults in most cases as well. I just fail to understand how anybody can be assured that just because there is a ban on children under the age of 13 that this ban can be enforced. I mean, anybody can say they're 13 years of age or over. If a kid is determined that they're going to go on this site because their peers are or for whatever reason, then they're going to indicate that they're over 13. I think it's just a ludicrous thing to even think that it could give anybody any type of comfort.

I'm wondering if you could talk a little bit about the other countries. You talked slightly about the U.S. and some of the safeguards they have in place. Are there other things in other countries we could look at?

As well, do you have any examples of social networks where children are specifically targeted and perhaps being used for commercial gain? And do you think kids themselves are concerned about their privacy rights?

**Dr. Sara Grimes:** There have been some developments and some recommendations in the EU. I'm not up to date enough on that to know where they are in that process. They did a huge study in the EU, which ended recently. Academics and a number of government agencies studied these types of issues with kids of various ages online in something called the EU Kids Online project. After the reports came out, I know that discussions started about industry guidelines and implementing new guidelines and implementing potential regulations. Where they are in that process, I'm not entirely sure, but that would be one place to look. I know they have been considering it, and they've also grounded a lot of what they've been doing in research, which is great.

In terms of examples of children being specifically targeted and used for commercial gain, one of the big problems of studying this area and these processes is that there's a lack of transparency. Data is collected and you can read the terms of service and you kind of see the data coming out in different places, but it's not always clear what the links are and how data is being transferred and how it's being used. The examples I've looked at to see how this process can work tend to be sites that actually sell the data to other companies and that are quite open about selling the data to other companies. They function as a social media space, but they also do data-mining and data-brokering in-house.

An example from a few years ago was that of Neopets, which is an online community for kids. They sold the market research they had done to various different companies and had an annual report in *AdAge*, which is a big advertising industry trade publication in the U. S. They would include surveys and pretty easy-to-identify market research strategies within the site.

A more recent example is Habbo Hotel, which is based out of Finland but is popular all around the world. Most of the people who use it are between the ages, I think, of 13 and 18, but they do have a significant number of users who are 11 to 13, as well. They offer a similar type of service, called Habbel, through which they package data and sell it to other companies. Through that service, companies can also hire them in advance to sort of spy on conversations that kids might be having about a particular product, and tell them not just what the kids are saying about the product but the larger context within which that conversation emerges—what kinds of likes those kids have, what areas of the site they are gravitating towards, what other things they talk about, what time of day they are there, where they plan to go after if they plan to meet up in real life, because a lot of kids who meet and communicate in social media actually do know each other in real life and go to the same schools and that kind of thing. It can be very detailed information.

The only reason we know how detailed they are and we know about these kinds of processes is that they're openly selling the data. But in many cases they're not selling the data. They're keeping it or they're selling it through more covert means, so it's not as obvious what's happening to it.

Are kids concerned about privacy? Definitely. There's been a lot of talk about the different concepts of privacy that kids have. I think this comes back to Mr. Andrews' comment earlier about kids being born in this age of Facebook, and not knowing any different type of environment and having pictures of themselves online before they're even old enough to go online themselves.

They may have slightly different concepts of privacy, but a lot of them are very similar to traditional concepts of privacy. In study after study, what comes out the most is that they're most concerned with privacy infringements that impact them on an immediate level: friends infringing on their privacy or parents infringing on their privacy or perceiving that their parent is infringing on their privacy. These abstract forms are at a length. They doesn't seem to impact them on that day-to-day basis. They are dealing with these privacy issues in ways that we have yet to fully appreciate. They might not seem as concerned about these things, but oftentimes they just don't really understand how they're going to impact them and where. Frankly, because so many of us also don't understand how those types of privacy infringements are impacting us and where, we're worried about what might happen, but we're not completely seeing the consequences yet. It's more difficult to find out how they feel about that.

● (1205)

There is a new study of Canadian children and youth that has come out just recently and has explored these issues. Increasingly, kids are even able to articulate these concerns about abstract privacy infringement, which I think is a really important development. They're learning about it more, they're experiencing it more, and they're able to communicate more about how it makes them feel and whether they feel their rights are infringed.

The sad thing is that I'm not sure if they feel there's an escape, a solution, or an alternative. There certainly isn't one being presented to them right now.

[*Translation*]

**The Chair:** Your time is up, because it includes the question and the answer.

Ms. Borg, you have five minutes.

**Ms. Charmaine Borg (Terrebonne—Blainville, NDP):** My thanks to the witnesses for being here today.

My first question goes to Mr. Israel. According to what I have read, when the commissioner makes recommendations about a privacy protection policy, some companies completely change their platforms so that the recommendations become redundant.

Could you comment on that? Could that justify the argument that the commissioner needs more powers to impose financial penalties?

[*English*]

**Mr. Tamir Israel:** Thank you. It's a very good question.

I think that in many contexts we do get a good level of compliance from industry, but the problem is that sometimes in the social networking context and the Internet context, some of the mechanisms that it takes to comply with the Privacy Commissioner's recommendation take a while to implement—to develop and to put in place. We've seen this in the United States with the Federal Trade Commission in a number of the privacy complaints they've looked at. We've seen it in Canada a little bit.

The problem is that the mechanism we have in place under PIPEDA is not very well suited for the Privacy Commissioner to have ongoing control of that issue. Forty-five days after they implement their recommendation, they're faced with a decision on whether to take the issue to the Federal Court—to start from scratch and to do it in the context of a trial, which is not a very flexible context to be in when you're trying to do privacy governance—or to enter into really undefined arrangements.

In one case we had, it was basically almost a contractual arrangement that was entered into with the party. In the United States you're seeing similar things, where it's a settlement agreement between the Federal Trade Commission and companies to do certain things over certain years. But there are not necessarily a very clear enforcement mechanism and a process in place to deal with those types of compliance processes.

● (1210)

[*Translation*]

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

Are there cases when companies completely change their platforms in order to avoid implementing certain recommendations? Is it a problem?

[*English*]

**Mr. Tamir Israel:** I would say that it's a problem, yes, but part of the problem is that it's a two-tiered problem. These sites evolve at such a rapid pace that it's hard to.... You need something more flexible, so that the Privacy Commissioner can adapt. Six months in Internet time is a decade in non-Internet time, so what you need is a process for the Privacy Commissioner to be able to adapt, in an ongoing manner, what the intent of their principle is. Because what will often happen is that by the time the response get implemented, it ends up doing the opposite of what it was intended to do, for example.

[*Translation*]

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

Mr. Kardash, do you want to comment?

[*English*]

**Mr. Adam Kardash:** May I offer a comment? Just by way of background, I've had the opportunity to represent companies across sectors in multiple investigations with the Office of the Privacy Commissioner of Canada. At least in my experience, once an investigation has been commenced, the companies always end up working out—or have worked out—a solution tailored to their business practices, but to the satisfaction of the OPC.

As I mentioned in my opening remarks, Commissioner Stoddart has been on record as saying that the mere threat of Federal Court action has been very effective. Nothing is more important to most companies—if not all companies—than their reputation. The prospect of being publicly named is something that they really want to make sure doesn't happen, so they comply.

[*Translation*]

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

Mr. Israel, you mentioned Acxiom as an example of a company that has gathered a large amount of data.

Should we be thinking of establishing principles that would limit the amount of data that companies are collecting? How could that be put into practice at the moment?

[*English*]

**Mr. Tamir Israel:** That's a very good question. I think it's something that really needs a lot of closer study.

The same issue is starting to arise in the child gaming context. The marketing materials used to be easier to get because companies would have their practices out in their marketing materials. If I were trying to figure out what a specific site was doing, I could pick up their marketing materials and see it in there, as Sara was saying. Now they've moved away from that. They don't have those marketing materials available any more, so it's not as easy to do.

It's the same issue as with the data brokers. It's not very clear to me what they're doing. Some of their marketing materials are available, so you can get a sense, but I think you need.... I don't have a solution. I think what's needed is a more in-depth investigation, with those data brokers at the table, that tries to get them to explain what their processes are.

What's been suggested is to just have a centralized place where individuals can ping these data brokers and do searches of these data brokers all in one place to see if their names are on there. Then you have, under PIPEDA, for example, a right to request an organization to give you everything they have on you. But you have to first know which organization to go to, what the organizations are. I don't want to send out 100,000 of these. If there are 100,000 data brokers, I want to be able to go to one spot, see who these are, send them requests, see what data they have on me, and then maybe correct any errors that are there.

In addition to that transparency mechanism, there's probably an analogous regulatory-ish mechanism that could be put in place that would talk to these organizations and get a sense of where their data's going, how it's being used, and where it's being collected from. That's a fact-finding type of expedition that I think would be really useful, but it's very difficult for individuals to undertake on their own.

That's a starting point.

● (1215)

[*Translation*]

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

I now recognize Mr. Butt, for five minutes.

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

[*English*]

Thank you very much, witnesses, for being here today. I think the other committee members have said it well, that we're learning a great deal today. I really appreciate your expertise in this area.

Let me run a concept by you and get your feedback on it. I'm going to call it, for lack of a better term, a reverse negative billing option as far as the privacy or consent form is concerned. Would it be possible, or do you see it working, that unless a user specifically gives consent for their private information to be held by the user—Facebook, Google, whoever it is—and then disseminated, versus their providing specific consent that it may be used...?

As I understand it now with the privacy policies, it basically says that they can use all this information for anything they want. You click "I agree". Nobody reads the 15 pages. You just click "I agree" because you want to sign up.

Can it work in reverse? Can we set it...whether through Parliament in our rules or laws, or through companies just getting together? I'm going to talk about your self-regulatory model in a second, as my follow-up question. Can we start to put pressure on these companies—and would it work—to have a privacy policy that works in reverse? For example, "You may not use any of my personal private information for any reason unless I specifically consent to your using that information". Is that viable? Would it even work?

**Mr. Tamir Israel:** I agree with what my colleague Mr. Kardash was saying before, that you do need a flexible framework in place. We do have a consent regime in Canada, so the starting point is that technically they do need my consent. It's a graduated consent regime, where the more sensitive the information is right now, under PIPEDA, the more explicit the consent you need to seek—in theory. The problem is that transposing that onto the social media context has been very challenging, just given the rate of evolution of these services.

So I think we have that to an extent. I think we would just need to maybe bolster it a little bit to make it more of an implemented reality.

**Mr. Brad Butt:** Do you see that as something that Parliament, through a law, through changes to the PIPEDA legislation, or in some other fashion...? Do we need Canadian law to enshrine that, or do you see that as something that industry could do through moral suasion, let's say?

**Mr. Tamir Israel:** I think a combination of the two. You need the principle in place under PIPEDA, and I agree with Mr. Kardash that PIPEDA has been very successful in setting in place a very broad, principled framework that the privacy commissioner has applied in a flexible manner, in a sort of co-regulatory manner, in the sense that the guidelines are issued and companies attempt to implement them, and there's discussion with industry and sometimes with other stakeholders on how to develop and apply those.

I think that's the proper mechanism, but the principle itself needs to be embedded in the statute, and then there needs to be a potential, at least, for a penalty for serious cases of non-compliance, clear cases of non-compliance, not borderline cases or something like that. Then, within that context, I think you can develop a co-regulatory framework where the principles get applied in a flexible manner. I think that's the way to go.

**Mr. Brad Butt:** Do the other witnesses want to jump in on this one before I ask about the self-regulatory...?

**Mr. Adam Kardash:** It's an excellent question. In international forums and global think tanks discussing privacy, one of the emerging issues focuses 100% on consent. The question is actually not whether it should be an express or an opt-in, as you were mentioning, or an opt-out form of consent; the question is more in a context of meaningful privacy protections. Is consent even the model of the way to go? Perhaps it's a way of robust user control, as mentioned by your colleague Mr. Calkins, in the context of broad and holistic privacy governance. For the meaning of that, again I refer the committee to the excellent joint guidance issued by the privacy regulatory authorities. It's very comprehensive, with over a hundred expectations for how to provide appropriate privacy protections in a balanced manner for business.

The issue is, once you focus just on consent as the trigger to get into a site or user-specific technology, it quickly becomes a meaningless apparatus in and of itself to actually enhance privacy protections, because once you receive that, you still have to address more radically the more broad set of concerns, and those become more important.

This is why internationally you're actually seeing a trend towards not relying as heavily on consent, as many current statutory frameworks do.

● (1220)

**Mr. Brad Butt:** Professor Grimes, did you want to speak? Not on that one.

Am I done?

[*Translation*]

**The Chair:** Yes, the time is up.

**Mr. Brad Butt:** Thank you very much.

**The Chair:** I recognize Mr. Boulerice, for five minutes.

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

My thanks to our guests for joining us today.

I would like to start with a basic question to all three witnesses. If I understand correctly, the business model of social media depends on collecting personal information that is then sold to companies that target people in order to sell them their products.

If we try to protect people's privacy and the personal information of those who use social media, are we not going against the very nature of the system, which is all about collecting information and then selling it to companies interested in having it?

[*English*]

**Dr. Sara Grimes:** I guess it depends on how you define social media—if you think of it purely as Facebook as social media, that's its business model and that's how it operates. I take a broader definition of social media, because the kinds of social media kids use include games and all kinds of different things.

A lot of the more successful online games for kids are subscription models. They pay a monthly fee. There's no real reason to do this additional data-mining. It's extra money, I guess, and extra insight into the market, but a lot of that could probably be done—in terms of insight into the market—with permission and consent and a more transparent process.

Take an example like Club Penguin. It's owned by Disney. It was a Canadian company, and there are still links to the Canadian company that founded it. It's a subscription model. Kids pay a nominal monthly fee to play it. It's enormously popular. They don't do third-party advertising, so there's not that explicit link, and any data mining they do is in-house. We don't know what that might be, but to say that data mining and selling the data is completely necessary for them to function is not at all true. They have tens of millions of players paying money every month for the opportunity to play.

I guess it would depend on the definition.

**Mr. Tamir Israel:** Just to be clear, Facebook doesn't sell data to data brokers. It actually uses the same kind of model. It's an internal marketing model where the information stays in-house, and if I were an advertiser, I'd pick the five categories of people I wanted to see my ads. So it's actually pretty good in that regard.

I think our Privacy Commissioner's finding on Facebook's practices actually held that to a certain degree they can do certain types of targeted advertising, because that is their business model and that's acceptable and everybody understands that. It's a question of where that line gets drawn, and then, when you start to get into more sensitive types of data, how you do controls around that.

As for these other types of data brokers, now we're talking about people I've never had any business or interaction with at all. They're collecting data that's either publicly available or through various other means I'm not necessarily involved in, and I think those are a little more questionable.

So I think there are different tiers of business models, and you need flexible approaches to address each of them—but I think there's room for improvement across the board.

**Mr. Adam Kardash:** I have nothing further to add, other than to say that the services are free. So they're supported, as reflected in the Office of the Privacy Commissioner's decision in the Facebook investigation, by certain practices and they were found to be in compliance with PIPEDA.

To the extent that your question relates to broader data practices involving advertising, the Office of the Privacy Commissioner of Canada has again shown leadership in coming out with specific guidelines dealing with online behavioural advertising. This is going to be worked in concert with a self-regulatory framework that's being developed by industry to effectively allow individuals to exercise choice in that context.

● (1225)

[*Translation*]

**Mr. Alexandre Boulerice:** My next question goes to Mr. Israel. It has to do with Acxiom, or with online data brokers. This is the first time that I have heard about them. I find it a little troubling.

Are there a lot of players like that? How do they get their information, their data, and who do they sell it to?

[*English*]

**Mr. Tamir Israel:** Sorry. Please say that again.

[*Translation*]

**Mr. Alexandre Boulerice:** I would like to know who these players are. Are there a lot of them? Where do they get their information from and who do they sell it to?

[*English*]

**Mr. Tamir Israel:** I would also like to know that.

There are a number of them. I think Acxiom is one of the bigger ones, and there are other examples. I think ChoicePoint has historically been an interesting one that was mining data from various sources and created profiles for law enforcement to use in the States.

There are a number of them out there of varying sizes, and that's part of the problem, in that it's hard to get a complete picture of where they all are and exactly how their data flows. Some of it is collected from the vast amounts of information that's now publicly available. In a social media context, I think that should be one of the factors we're taking into account when we're deciding where privacy defaults should be set, and those kinds of things.

As for another potential avenue for information to flow to these databases from sites like Facebook or others, though I don't want to single out any specific companies, there are a lot of third-party applications that get put onto Facebook, such as FarmVille and games like that.

I think it's actually a violation of Facebook's terms of use to sell information further downstream to these brokers, but it's not very clear exactly how that's enforced. I think technically Acxiom could make its own application and put it on Facebook.

[*Translation*]

**The Chair:** Thank you.

[*English*]

**Mr. Adam Kardash:** My one comment is that it's important to highlight that the companies that have been mentioned are U.S.-based companies, and the extent to which they even carry on in Canada is something that's in question. If they did, they'd be subject to a considerable set of requirements that would curtail the activities they would otherwise be able to do in the U.S.

So it's important to keep in mind that those aren't Canadian-based companies carrying on these types of activities; it's U.S. companies that have been mentioned.

[*Translation*]

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

Mr. Dreeshen has the final five minutes today.

[*English*]

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

Thank you for attending, witnesses. It's been very interesting.

Mr. Boulerice was just speaking of something I was trying to get my head around, that being, who are these data brokers and how are they making their money? I suppose as a committee that's something we can drill down to, and if you have any other information, I'm sure we'd like to get hold of that.

Mr. Kardash, one of the things you had mentioned earlier as well was the Alberta and the Alberta-B.C. documentation and the expectations. I'm sure our committee would appreciate getting that contact information so we can also review that.

Another thing you also talked about, Mr. Kardash, in your four points was the constitutional impact that would have to be reflected upon. So I wonder if you could expand on that first.

**Mr. Adam Kardash:** Okay.

PIPEDA is grounded upon the constitutional authority in the second branch of the federal trade and commerce power. When initially it came into force, there was some question about the constitutional validity. That dropped off, for reasons unknown to myself.

Very recently, the Supreme Court of Canada issued a decision in the context of a national securities administrator and the movement to establish that. In the context of considering the establishment of a national securities administrator, the Supreme Court of Canada unanimously declared that the reliance on the trade and commerce power would be unconstitutional.

This, at least for those of us in the privacy arena, led to a natural question about the extent to which it's applicable to PIPEDA, and especially in the context of an environment where more enforcement powers might be provided to the Office of the Privacy Commissioner of Canada.

It's for constitutional experts to consider. I'm no constitutional expert. It's just that this was an important decision issued by the Supreme Court of Canada that is worthy of consideration in the context of any legislative initiative, in particular any that would expand enforcement powers, at least in my view.

● (1230)

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

Ms. Grimes, you went through four different points. You were talking about child-specific regulations on data, clearer articulation of informed consent, and I believe freedom of expression of rights, as well as leadership and enforcement.

You also spoke of some Canadian businesses that have really shown some brilliant practices. I'm just wondering if you could expand on that for a minute.

**Dr. Sara Grimes:** Yes. I'm really glad you asked that question, because I love talking about these good examples as opposed to some of the scarier and more extreme practices that can be found.

Some examples of great Canadian social media companies include Storybird, which is Ottawa-based, I believe, but they have offices in Toronto as well. Their privacy policy is written for kids and parents. It explains all kinds of things. It even talks about the things that they don't do—such as data collection practices that are found on other sites that they don't do—just as a way of making sure that they distinguish themselves from those practices. Storybird is a social media site that allows kids, parents, and teachers to create picture books and trade them. It's actually quite vibrant. It's being used in schools, so it's really great to see that they're all seeing this really great privacy policy.

Another example is Frima Studio, which is Montreal-based. They create online games. I watched them actually struggle for quite a few years with their privacy policy in terms of service, to the point where it got to this child-friendly language, very well articulated, in an explanation of all kinds of very complicated legal processes. Again, they also explain the things that they didn't do, as well as the things that they did do.

I guess a last example would be zinc Roe, a Toronto-based company. They create apps. They've been really at the forefront of engaging with academics, child advocates, and parents in terms of figuring out what the best practices are for how to deal with information that toddlers are creating and sharing, and information that parents are creating about their toddlers. It's a very sensitive area. They're very much engaged and involved in coming up with these very ethically informed best practices.

Those are three examples. I would love to see them more involved in these debates, because they have great ideas and they're actually putting them into practice.

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

[*Translation*]

**The Chair:** Your time is up. That concludes the testimony from our three guests today. Thank you for being here.

I will suspend the session for a few minutes and then we will come back to discuss future committee business.

● _____ (Pause) _____

●

● (1235)

**The Chair:** We are now ready for the second item on the agenda.

Mr. Warkentin, do you want to say something?

[*English*]

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

I'd just move that we move into camera for committee business.

[*Translation*]

**The Chair:** Mr. Warkentin has moved a motion to continue in camera. As the motion is not debatable, we will have a recorded vote.

(Motion agreed to: yeas 7; nays 4)

[*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**