HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 059 • 1st SESSION • 41st PARLIAMENT

EVIDENCE

Tuesday, December 11, 2012

Chair

Mr. Pierre-Luc Dusseault

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, December 11, 2012

● (1530)

[*Translation*]

The Chair (Mr. Pierre-Luc Dusseault (Sherbrooke, NDP)): Order, please.

We will begin the 59th meeting of the Standing Committee on Access to Information, Privacy and Ethics and continue the study on privacy and social media.

Today, we are fortunate to have two witnesses with us. First, we have a representative from BlueKai, Mr. Chapell, who will make a 10-minute presentation. Afterwards, we will be able to ask him questions. We will also hear from the Privacy Commissioner who is visiting us for the second time. She will summarize what has been said so far, since this should be the last meeting on this study.

Without further ado, I yield the floor to Mr. Chapell for ten minutes. As I already said, we will then have an opportunity to ask him questions.

Mr. Chapell, I want to thank you for joining us. The floor is yours.

[*English*]

Mr. Alan Chapell (Outside Counsel, Privacy Officer, BlueKai Inc.): Thank you, Mr. Chairman.

Mr. Chairman and members of the committee, thank you for inviting BlueKai to testify at this timely and important hearing. My name is Alan Chapell, and I am the outside counsel and privacy officer for BlueKai Incorporated, a digital data company with headquarters in Cupertino, California.

It is an honour to appear before this committee. I am pleased to describe BlueKai's business and share with the committee some of the privacy innovations we've developed at BlueKai.

BlueKai's mission is to build the world's first complete enterprise platform for data-driven marketing with the utmost attention and diligence to ensuring consumer privacy. We offer a data management platform that enables advertisers to collect, store, and utilize anonymous consumer preference data. Since our founding in 2007, BlueKai has embraced the privacy by design ideals championed by Information and Privacy Commissioner Dr. Ann Cavoukian. We recognize the importance of incorporating privacy into our products and services and have fostered a culture of protecting consumer privacy interests from day one.

BlueKai's platform enables businesses to utilize pseudonymous bits of marketing data for online behavioural advertising and analytics purposes. The platform allows businesses to create target audiences based on a combination of their own data and third party data in order to reach their target audiences across third party advertising networks and exchanges. The platform also helps those businesses to measure with accuracy which campaigns performed in order to refine media buys and advertise creatively over time.

The marketing data stored on the data management platform is generally governed by the privacy polices of our clients. BlueKai offers guidelines to help ensure that our clients understand the applicable privacy law and self-regulatory standards.

BlueKai also offers a data exchange that enables businesses to utilize pseudonymous third party data for their digital advertising campaigns. We take steps to ensure that the third party marketing data listed on the BlueKai Exchange meets or exceeds applicable privacy law and self-regulatory standards.

BlueKai is a board member of the Network Advertising Initiative, a coalition of more than 95 leading online advertising companies committed to shaping and enforcing responsible privacy practices for online behavioural advertising. We are also a member of the Digital Advertising Alliance, the industry-wide self-regulatory program for online behavioural advertising. We've been active in the behavioural advertising self-regulatory movement in North America, Europe, and the rest of the world since our founding.

We understand that a similar behavioural advertising self-regulatory program is being developed in Canada. Further, this program's privacy requirements are generally in harmony with the policy position on online behavioural advertising offered by the Office of the Privacy Commissioner of Canada. BlueKai has historically been a leader on the move to industry self-regulation. We aspire to continue that pattern and be one of the first companies to participate in the Canadian self-regulatory initiative when it is launched.

Last but not least, BlueKai participates actively in the World Wide Web Consortium's tracking protection working group to develop a browser-based do-not-track standard.

In addition to being active participants in industry self-regulation for online behavioural advertising, BlueKai has a history of innovating on privacy issues. I'd like to share two of those privacy innovations with the committee today.

The first is the BlueKai Registry. BlueKai was one of the first digital marketing companies to provide consumers with enhanced transparency by offering access to marketing data via the BlueKai Registry. The BlueKai Registry, which is available at BlueKai.com, brings transparency to consumers by allowing them to see what preferences are being stored via the BlueKai cookies on their computer.

Furthermore, consumers may also control their anonymous profile by managing their topics of interest. We strongly believe that offering consumers this level of transparency and control builds consumer trust. We've seen that in practice; relatively few consumers who visit the BlueKai registry actually opt out from further use of their preference data. This suggests to us that consumers who understand BlueKai's practices are generally less concerned by them.

● (1535)

The second innovation is the BlueKai opt-out protection tool. One of the challenges to offering opt-out choice in an online advertising context is that cookies serve a dual purpose. In other words, cookies are used to store marketing data and to record an Internet user's opt-out choice.

When Internet users delete all of their cookies, their opt-out choice may also be deleted. The Office of the Privacy Commissioner of Canada has proposed that opt-out choice is appropriate for most forms of online behavioural advertising; however, the Privacy Commissioner also recommends that such choice be made persistent. This recommendation is in line with the recommendations made by regulators across the globe. BlueKai has taken steps to meet those recommendations with the BlueKai opt-out protection tool.

Utilizing some open-source code, BlueKai developed a Firefox browser plug-in that was designed to protect user opt-out choice even when users have deleted their Internet cookies. This code was licensed to the Network Advertising Initiative, so all NAI member companies were able to leverage the opt-out protector technology. This opt-out protection concept was further embraced by the Digital Advertising Alliance and expanded to include most major Internet browsers.

We're proud that our hard work was able to help BlueKai and other online behavioural advertising companies to protect consumer privacy choices. We take privacy very seriously at BlueKai and are happy to have had the opportunity to share some of our privacy innovations with this committee.

I'd be happy to answer any questions.

[*Translation*]

The Chair: Thank you.

I will now yield the floor to Mr. Angus for seven minutes.

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

[*English*]

Thank you very much for coming today. We really appreciate your participation in this study.

As you're probably aware, we're trying to get a sense of the world of big data and how it plays in with social media so that when we come forward with possible recommendations, we're not proposing reactive legislation that would actually interfere with the development of the new opportunities out there and that will also, as well as we can in our position as MPs—which is very far from the cutting edge—try to ensure we have some basic standards of protection, particularly on the privacy rights of Canadian citizens.

I'd like to ask you a first question. Does BlueKai gather data on Canadians?

Mr. Alan Chapell: We do have some business in Canada. It is not a large lion's share of the business that we currently do, but there is certainly some data collected on Canadians.

Mr. Charlie Angus: Thank you.

We met with Acxiom last week. They said we were too small a market, which we didn't take personally. We were actually kind of relieved generally, I think, that they only were interested in our phone books.

One of your founders, Omar Tawakol...?

Mr. Alan Chapell: Yes: Omar Tawakol.

Mr. Charlie Angus: He says, “Right now, data looks like black, gooey material. Oil was to the industrial revolution as data is to our information economy.”

Do you mine this black gooey material, or do you process it? What's your role with the goo that is data?

Mr. Alan Chapell: I think he is making the analogy that data can be very valuable. It can be very helpful to consumers. It can foster innovation.

Our primary business is a data management platform, which really provides the plumbing for the oil pipeline, I guess, if we're going to extend the analogy.

Mr. Charlie Angus: Do you congregate these various points of data into profiles or do you take what data is there and then make sense of it?

Mr. Alan Chapell: I think we do a little bit of both. There is certainly an analytics and analysis component to the platform, and certainly the data exchange product does obtain consumer preference data.

Mr. Charlie Angus: All right.

I'm interested in the opt-out clauses and certainly in the issue of cookies. I turn my cookies off, but sometimes I can't go onto a website—Firefox or other browsers—unless I turn the cookie on, which means I'm actually allowing myself to be tracked. I don't really feel that it's something I've agreed to; I've agreed to go to the website, and I need to turn the cookie on. How important is the cookie in terms of being able to track what I do online?

● (1540)

Mr. Alan Chapell: The cookie is essential for a number of things online: certainly the ability to track, the ability to remember a particular browser on a particular page when it visits the next page in order to provide what they call "state", so that there's some ability for a continuous user experience.

Mr. Charlie Angus: That means that if I go from one site to another to another, it's actually possible to track me and say that I was here, I was there, and then I was there. It starts to form the pattern.

Mr. Alan Chapell: It's certainly possible. What that would presume is that the same company was dropping cookies on the first site you visited, and then the same company was dropping cookies on the second site you visited, and the same company was dropping cookies on the third site you visited.

Mr. Charlie Angus: But a data broker could take the information from the three different points and correlate it. This wouldn't be necessarily the one cookie on Amazon or another commercial site, but these points of data actually can be congregated into a profile.

Mr. Alan Chapell: I think the data points can be congregated not necessarily into one continuous profile knowing that you've been on website X, website Y, and website Z, but if website X is a finance website, it's very possible that there may be an indication that the browser has visited a finance website. If the next one is on a travel website, there's a possibility at least that a cookie indicating a preference for travel would be dropped on the browser subsequent to that.

Mr. Charlie Angus: A *New York Times* article on BlueKai was really interesting. It said:

> BlueKai's business model stands or falls on the idea that our digital profiles are anonymous at the time they're auctioned off. In fact, computers can link our digital profiles with our real identities so precisely that it will soon be hard to claim that the profiles are anonymous in any meaningful sense.

With my tracking experience of going to a financial adviser, trying to find a place to go in Cuba, and how much booze I bought for the Christmas party because I was looking at various prices, that's not anonymous data. That's fairly easy to link to me as a person. Is that correct?

Mr. Alan Chapell: My first answer would be that BlueKai doesn't engage in any type of profiling regarding alcohol usage, so it's important to make that clear.

Mr. Charlie Angus: Thank God.

Mr. Alan Chapell: There are a number of segments that we consider off limits.

Mr. Charlie Angus: But you do provide that profiling, and it goes to an actual person. It's not just aggregate data.

Mr. Alan Chapell: It goes to a specific Internet browser—

Mr. Charlie Angus: Right.

Mr. Alan Chapell: —which may or may not relate to a specific individual, because computers are shared or Internet browsers are shared.

Mr. Charlie Angus: We had Google here, and they were saying that with their new Chrome platform—which I have yet to use, because it won't work on my Mac, but that's a side story—they basically allow complete stealth operation. How does that affect BlueKai, if the browsers start to opt in to give users the ability to go under the surface without being tracked? Is that going to affect your business model at all?

Mr. Alan Chapell: Most of the major browsers have offered some form of stealth for a couple of years. I think some of them call it "incognito". I think each browser has its own nomenclature for it. Those have been in existence for a number of years. To the extent that it provides users with some comfort that those Internet browsing sessions will be subject to the incognito rules, I think that's a good thing. We haven't seen stealth or incognito having a significant impact upon the BlueKai business to date.

[*Translation*]

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

I will now yield the floor to Mr. Calkins for seven minutes.

[*English*]

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

I'm listening with great interest about your platform. You answered a couple of questions that I had as you went on with your conversation.

I want to talk a little bit about cookies. Just so I'm clear, your company is a data aggregator. Is that right?

Mr. Alan Chapell: I think that's a fair description.

Mr. Blaine Calkins: Then you use that aggregate information and provide third party advertising directed back to a particular computer based on the cookies that are in the cache or in the cookie file that is commonly used by whichever Internet browser might be used on that computer at that particular point in time.

● (1545)

Mr. Alan Chapell: I think that's correct, sir, with the caveat that BlueKai isn't using this data. We provide a platform that allows our advertising clients to utilize that data.

Mr. Blaine Calkins: Who has that data?

Mr. Alan Chapell: The data is stored by BlueKai.

Mr. Blaine Calkins: The data is stored by BlueKai, but there's data also on the local machine. That's there in both cases.

Mr. Alan Chapell: Yes, sir.

Mr. Blaine Calkins: I can write an app. I used to do this for a living, so I can write an app that will create a cookie and store it on a computer, and every time somebody puts information in a form—first name, last name, address, and so on—that information is stored on a cookie. The reason it has to be stored on a cookie is that a web page is static, not dynamic, even when you're using dynamic HTML, or whatever it happens to be.... Is this language that you and I both understand?

Mr. Alan Chapell: Yes, sir.

Mr. Blaine Calkins: For the sake of edification, the reason cookies are used is that they're a necessary tool. It's not a client-server application. It's a static page, making a transaction with whatever other servers are out there across the Internet at that time. The cookie is there simply as a vehicle to store the information. It's a tool, sometimes temporary and sometimes permanent, for maintaining profiles, user information, or whatever it happens to be.

This is why, when we log back on to a number of different websites, the information that we were there last time is already automatically preloaded into that web page. This way, we don't have to constantly keep doing it. We get prompted as users from time to time if we want Internet Explorer to save the information for future use. That information's stored in a cookie. I understand that.

What I need to know from your perspective is this: you have this opt-out protection tool, which relies on a cookie to keep track of the bit or the signal or whatever it is that says they've opted out, yet as my colleague Mr. Angus brought to our attention, if he chooses to turn the cookies off and delete the cache or the history, and all of the cookies are wiped out, you have no knowledge of that opt-out on the machine.

Is that correct?

Mr. Alan Chapell: When the opt-out protector tool is not in the user's browser, then the answer to that question is yes. We saw that as an issue in the marketplace, and that's one of the reasons that we created the BlueKai opt-out protector. It's a browser plug-in tool.

Mr. Blaine Calkins: It's a plug-in.

Mr. Alan Chapell: Even when users delete their cookies, the opt-out cookie will not delete.

Mr. Blaine Calkins: Is it a Java plug-in, or what kind of a plug-in is it?

Mr. Alan Chapell: I believe it's a Java browser plug-in.

Mr. Blaine Calkins: It's a Java plug-in. Okay.

You said you made the source code public.

Mr. Alan Chapell: We did. We took a source code—

Mr. Blaine Calkins: So anybody...

Mr. Alan Chapell: —provided by Google....

Mr. Blaine Calkins: —anybody could reverse-engineer this. Anybody could take a look at it, and anybody who has the experience could look at the code and understand the nature of what's happening there. It's a transparency mechanism for BlueKai, right?

Mr. Alan Chapell: Well—

Mr. Blaine Calkins: It creates a standard platform that everybody can use and have access to.

Mr. Alan Chapell: Correct.

Mr. Blaine Calkins: That's good.

Getting back to the issue of privacy, what is it you're offering that sets you apart? It doesn't sound to me like you're offering anything terribly different from what's already available out there for any data aggregator, except you have this registry, this enhanced transparency, that allows people to see what's there. How is that new or different? What are you doing that sets the bar above or beyond what everybody else is doing in the marketplace?

Mr. Alan Chapell: My understanding is that there are fewer than 10 registries in the marketplace right now. Correct me if I'm wrong.

Mr. Blaine Calkins: No, I'm—

Mr. Alan Chapell: There may be more. Google has one. Yahoo has one. I believe Microsoft has one. There might be three or four other companies that have one. BlueKai has one. This level of transparency is not something that I would characterize as being common in the marketplace.

Mr. Blaine Calkins: Is the ability of the user to directly engage in that registry what sets you apart?

Mr. Alan Chapell: We think that's an example of a privacy innovation.

Mr. Blaine Calkins: I'm not coming after your organization. I understand the value of it. I totally get the freedom. People want to be free to do what they want to do on the Internet and have their say, but they are also concerned about their privacy.

Can you enlighten the committee on the technical capabilities that would allow users to visit a website they couldn't otherwise go to if they chose to turn their cookies off or if they chose not to sign on to a user licence agreement?

I've had some people before this committee say how difficult it would be to provide a platform that allows users preferences based on the level of security and the level of interaction with the company. I don't think that it would be all that difficult to do.

Do you think that would be an onerous thing to do? For example, instead of a one-button, select-all agreement to all the terms and conditions of an end-user licence agreement, could the industry have specific parts of that agreement agreed to and others not agreed to and still provide the user with the experience of visiting a website?

● (1550)

Mr. Alan Chapell: Well....

Mr. Blaine Calkins: It's a tough question.

Mr. Alan Chapell: It's a really tough question. We don't provide any end-user licence agreements.

Mr. Blaine Calkins: I understand that.

Mr. Alan Chapell: Other than BlueKai.com, we don't own or control any websites. Additional granularity in privacy statements would be a really helpful thing, as it would be in end-user licence agreements.

The layered privacy notice that Martin Abrams over at Hunton & Williams and a number of others have proferred over the years is a positive step forward, but there's a wrinkle: if you provide a summary at the very top of what your privacy practices are and then give the legalese below, a regulator might think the summary is out of harmony with the legalese. At least in the United States, there's potential to have a regulatory issue. That's one of the things that some companies find challenging.

[*Translation*]

The Chair: Thank you, Mr. Calkins. You're out of time.

[*English*]

Mr. Blaine Calkins: Are you sure? We're having a great conversation here.

Thank you very much.

[*Translation*]

The Chair: I will now yield the floor to Mr. Andrews.

[*English*]

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

Welcome.

Maybe you can just explain to me your platform and how it is anonymous. You have this information about a person, but it is still anonymous, and the advertisers are attracted to this anonymous information. Explain that to me. I am sort of losing what your model is there.

Mr. Alan Chapell: It's a pseudonymous model in which we know a certain profile corresponds with a particular browser. That browser may be used by one person. That browser may be used by multiple people. The computer may be used by multiple people. If you were to visit, say, a travel website, a cookie might be dropped onto your computer by BlueKai or another company. That cookie does not say, for example, Alan Chapell. That cookie just says, “interested in travel to Hawaii”. There is no way to identify the user based upon “travel to Hawaii”.

I imagine a vacation in Hawaii would look pretty good to many in this room right now .

Mr. Scott Andrews: Advertisers are attracted to this model because...?

Mr. Alan Chapell: In some respects, it goes back to the basic tenets of direct marketing. If it's more likely that a particular ad is going to be more interesting to a particular browser, the advertiser is more willing to pay a website publisher for placement of that ad. That way, the targeted advertising actually funds a good deal of the content that consumers enjoy for free.

Mr. Scott Andrews: You provide that browser information to the company that wants to do the advertising. Is that correct?

Mr. Alan Chapell: We provide a platform that enables those advertisers that advertise online to store that data and then analyze and utilize it to increase the intelligence of future digital media buys.

Mr. Scott Andrews: Is there any way to link up the data you have with an individual offline? Is that possible? If the advertiser got the data, and then got it from somewhere else with the person's name attached, could the two be linked?

Mr. Alan Chapell: In these types of discussions, you want to separate what is theoretically possible in certain instances in a lab from what is practicable from a business standpoint. One need only look back a couple of years to, I think, America Online, which inadvertently released some search data. It was such a large file that a reporter was able to identify a number of individuals from a list that numbered, I think, in the millions. That was with a fair amount of work. Since then, I think the industry has taken additional steps to make it even more difficult to potentially identify a particular person. In technology, I suppose one can never say it's impossible, but in the case of BlueKai and the way our data systems are set up, I think we're very close.

● (1555)

Mr. Scott Andrews: Thank you.

[*Translation*]

The Chair: I now yield the floor to Mr. Carmichael.

[*English*]

Mr. John Carmichael (Don Valley West, CPC): Thank you, Chair.

Thank you, Mr. Chapell, for being with us today. I am getting a quick education from my colleague.

As you know, this study has been going on for some time. We have been trying to clearly understand our role as legislators in ensuring that consumer privacy is paramount. Through this study, we have come across a number of different areas that are very concerning, and there have been others about which we have been told it's best to just leave the industry alone, because with any more regulation we would stifle growth and employment. We're trying to find a fine balance in terms of where we belong in this whole process and at the same time ensure that consumer privacy is critical.

As you know, we have met predominantly with social media companies. I wonder if you would agree that the social media companies will push the edges of the envelope to the extent that they are able to until such time as a regulatory process says, “Enough.” Would you agree that is a fair statement, or am I overstating it?

Mr. Alan Chapell: I think it's safe to say that social media companies are participating in a developing culture regarding privacy. For example, I've been focusing on privacy for almost a decade. From a privacy standpoint, the notion of providing a website with a list of all your contacts and the events you happen to be going to and pictures of friends would have been unthinkable 10 years ago, yet today it is fairly widespread. Even the initial news feed was fairly controversial when Facebook offered it, and a number of folks screamed that this was a privacy invasion.

Both from a legislative and a regulatory perspective, it's a delicate balance to define the balance between stifling innovation and protecting consumer privacy interests. Fortunately in Canada, while I don't claim to be an expert in Canadian privacy law, I do know that a pretty comprehensive framework is in place already, and a self-regulatory program is going to be launched within the next several months.

From my perspective, it would be a very good idea to see how that program develops prior to taking proactive steps. At least give the industry the opportunity to demonstrate that this is in the consumer's interest.

Mr. John Carmichael: Hopefully if I've got enough time I'll come back to that before we finish, but I'm sure some of my colleagues today will pursue that line.

When you talk about the preference data and the privacy constraints around BlueKai, as the data drop into your data vault —for lack of a better term—and consumers determine they don't want their information out there anymore for whatever reason, when they push that opt-out button on that cookie, I read somewhere there's a six-month window, I believe, before that data is deleted. I'm not sure if that's accurate; you can correct that.

When I've opted out at my choice with my data—this is the information being stored at BlueKai or any other aggregator—am I correct in understanding that the data is fully deleted?

Mr. Alan Chapell: It is. I think when you're referring to six months, that's BlueKai's data retention period, but that's a separate thing from the opt-out period.

Once a user has hit an opt-out mechanism and a BlueKai opt-out cookie has been dropped, that effectively replaces the other BlueKai cookies and zeroes out that particular record.

● (1600)

Mr. John Carmichael: So the history that I've been aggregating in BlueKai over the period of time that we've been friends is completely removed?

Mr. Alan Chapell: I think it's safe to say that the opt-out cookie removes any targeting and preference data existing on that computer for future ad targeting.

Mr. John Carmichael: Are we back to the anonymous now, and the data being retained for the advertising media preferences, etc.?

Mr. Alan Chapell: I think to the extent that data is stored over a period of time by, say, an advertiser advertising in a digital format, the pseudonymous data will be maintained over time. The opt-out is typically forward-looking, and in the future they're no longer going to conduct online behavioural advertising.

I think that to destroy all data retroactively becomes a pretty significant challenge. There are people who are far more articulate than I, but I might point the committee to some of the discussions going on in the European Union regarding the right to be forgotten.

Mr. John Carmichael: Right.

How is my time, Chair?

The Chair: You still have 45 seconds.

Mr. John Carmichael: In our role—and we are going to be completing our study shortly—how would you advise us, from a recommendation perspective, in terms of what we should be looking at or be thinking about in terms of maximizing our effectiveness in protecting our consumers—Canadian consumers, specifically—in the use of their privacy?

Mr. Alan Chapell: Allowing the self-regulatory program to continue to develop, I think, would be a very good start. Then I would suggest regular interaction, whether that's strictly the Office of the Privacy Commissioner or whether this committee also gets involved, or both, but I think a regular check-in—I don't want to say a report card—might be a good way for this committee to continue to have oversight on the development of the self-regulatory program.

These things tend not to happen overnight. I have some experience with that in the United States, but I think that—

Mr. John Carmichael: We're moving in the right direction?

Mr. Alan Chapell: We're moving in the right direction.

Mr. John Carmichael: Thank you very much.

[*Translation*]

The Chair: Thank you, Mr. Carmichael.

I now yield the floor to Ms. Borg for five minutes.

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

This discussion is very useful, and I want to thank our witnesses for joining us today.

My first question is about the clients who use your program and services.

How can an Internet user determine whether a specific company uses your services to then be able to go on your website and say that they no longer want to be subject to certain provisions? Is that information provided somewhere? Do Internet users have access to that information?

[*English*]

Mr. Alan Chapell: We're seeing more and more Internet users download their own transparency tools. Ghostery is one that comes to mind, but I believe there are others. They're browser-based plug-ins that tell an Internet user which cookies are being dropped by which companies on the websites that they visit. Certainly, users can be provided with that mechanism with some additional transparency. We're seeing more and more Internet users utilize those exact types of tools.

Moreover, in the industry self-regulating program—and here I'm talking about the United States—there are two websites. One is called networkadvertising.org and the other is aboutads.info. Both of those websites enable users to opt out from all member companies.

Again in the United States, it's probably worth noting that we're seeing more and more forward-looking little icons on digital advertisements that are being targeted with online behavioural advertising data. From the user's perspective, looking at that little dot on the advertisement may not let that person know exactly which company is targeting them, but it does provide a mechanism for them to understand a little bit more about the practice of online behavioural advertising and then let them go to the opt-out page.

● (1605)

[*Translation*]

Ms. Charmaine Borg: Thank you.

So, if I have understood correctly, it is up to the user to use those tools to make that determination.

My next question is also about your clients.

When you sell your products or contact a client, do you encourage the protection of personal information?

[*English*]

Mr. Alan Chapell: Yes, we do.

I find myself involved in many, if not most, client interactions, helping to educate companies about what the privacy rule set is. Some of that depends on the jurisdiction and some of it depends on the type of data that's being utilized, but we take that very seriously. We see one of our roles in the marketplace as being the ones to help educate clients on what the rules of the road are for privacy.

[*Translation*]

Ms. Charmaine Borg: During your presentation and when answering my question, you talked about principles that have to be applied.

Could you elaborate on the principles you encourage, both as a member of the associations you mentioned and as a company that uses that data?

[*English*]

Mr. Alan Chapell: Sure.

I'm going to talk mostly about the United States. Many of these concepts are certainly working in other jurisdictions.

The first organization I mentioned was the Network Advertising Initiative. It's an industry trade association that's been around for about 12 years. The organization is made up primarily of what we call the Internet intermediaries: the networks, the platforms, the exchanges, and the data companies. These are the entities that sit in between a website publisher and an advertiser. They help facilitate the delivery of that.

With those companies, historically the challenge has been that since they don't control the ad and they don't control the website, it's difficult for those companies to push privacy standards out into the rest of the ecosystem. Those privacy standards involve notice, transparency, opt-out choice, and a rule set around what we call "sensitive data".

When I refer to the Digital Advertising Alliance, I'm referring to what is more of a broad coalition of industry associations, which includes the Network Advertising Initiative. However, it also includes the online publishers, the online advertisers, and the digital advertising agencies.

The goal of the Digital Advertising Alliance is to make sure that all the privacy standards are harmonized within the business ecosystem.

[*Translation*]

The Chair: Thank you, Ms. Borg. You're out of time.

I now yield the floor to Mr. Butt, for five minutes.

[*English*]

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

Thank you, Mr. Chapell, for being here for the committee today.

Would you say you're fairly well versed in the Privacy Commissioner's mandate as it now stands in Canada, and in what her roles and responsibilities are and what the general interaction is with the business community—probably with many of your clients—and so on? Would you say that you're fairly well versed in what her role is currently?

Mr. Alan Chapell: I believe I'm fairly well versed.

Mr. Brad Butt: Given that, and given some of the things we're looking at as a committee—her role and the interaction—one of the concerns I have is that sometimes government, even though it may be with the best of intentions, tends to overregulate or to set parameters that actually stifle innovation and creativity.

One of my biggest concerns about social media and so on is that the technology changes so rapidly. I'm not always quite sure that government can keep up with the rapidly changing things that are going on in social media and related sectors.

From your testimony, it sounds as though you would say that your organization is pretty much operating in a more self-regulatory environment, that you're trying to do your corporate best to make sure you're respecting privacy issues, and that you're operating in an appropriate environment, etc.

Is it a strong enough model, in your opinion, to make sure we're all endeavouring as well as we can to protect people's personal privacy while also making sure that the people who are more expert in keeping up with the technological change can react to it a lot faster than we, as parliamentarians, can in trying to come up with laws and chasing after things have already happened? Do you have any more advice in that regard for us?

● (1610)

Mr. Alan Chapell: I agree with everything you just said.

I might add that the challenge with creating legislation in a quickly changing technology environment is the proverbial law of unintended consequences. It is generally thought of as a bad idea for the government to pick winners or losers in an emerging media, or really in any marketplace. The challenge with just about any type of legislation is that, almost by definition, it's outdated by the day it's enacted.

The beauty of self-regulation, if there's an adequate enforcement mechanism, is that it can continue to grow and morph around the innovation that's going on in the marketplace.

Mr. Brad Butt: Has BlueKai had any direct interaction or involvement with the Office of the Privacy Commissioner in Canada, either through its contacting you and saying it had a concern over something or it had heard something or somebody had made a complaint to it about the organization? Have you had any interaction like that with our Privacy Commissioner in Canada?

Mr. Alan Chapell: We have not directly.

I believe there was some interaction about two and a half years ago. I chair the privacy committee of a group called the Mobile Marketing Association. We were building out some standards a couple years ago, and I believe there was some interaction. It was not directed interaction on my behalf. That's just so you know that there was at least some interaction going on there, but we have not received a complaint.

Mr. Brad Butt: Was that more to get some advice or that the office was offering some public education to your organization? Were you seeking some advice from the commissioner's office in drafting some guidelines that the industry itself could look at using? Was it more as a resource to your organization? Was that the primary role at that time?

Mr. Alan Chapell: Yes, it was. I think the office was kind enough to offer some of their insights to the Mobile Marketing Association.

Mr. Brad Butt: Did you find that to be a helpful role for that office? Was that helpful to you folks in coming up with some guidelines? To go back to the self-regulatory regime, were our Privacy Commissioner and her staff able to provide good, helpful advice to you, to help you craft the model that you're using?

Mr. Alan Chapell: Absolutely.

To be clear, though, I did not have direct intervention; there were folks on the team. I mean, in any multi-stakeholder process there will be a number of groups that interact. I believe the interactions were very valuable.

Mr. Brad Butt: This is my final question, Mr. Chair, before I turn it over.

This relates to a trip to Washington by some of the committee members. We met with some excellent organizations, including the FTC and others.

From your perspective, is there anything in the United States that they may be doing well that we could learn from? Is there any advice from your interaction as a company there versus here that we could learn from that you think is particularly helpful, or is it true what we heard from a lot of the organizations that we met with—that in this area Canada is actually quite a bit ahead of the United States in a lot of respects?

Mr. Alan Chapell: I think I would agree with the latter. In some respects, I think, we could learn from what you folks in Canada are doing.

In the discussions around self-regulation for online behavioural advertising, to my understanding—again, this is not direct, but I've talked with a number of folks who were involved—the discussions were much less contentious. There was a recognition that there needed to be compromise on all sides.

I feel very confident that the net result will be a program that finds the right balance. Sometimes in the United States we haven't always met that goal.

[*Translation*]

The Chair: Thank you, Mr. Butt.

Mr. Chapell, I want to thank you on the committee's behalf for your willingness to meet with us and help us with our study.

We will suspend the sitting for a few minutes. We will then hear from the Privacy Commissioner.

Thanks again.

● (1615)

[*English*]

Mr. Alan Chapell: Thank you, sir, and thank you to the committee. It was an honour.

[*Translation*]

The Chair: We will continue our meeting.

I want to thank Commissioner Stoddart and the two people accompanying her—Ms. Bucknell and Ms. Bernier—for joining us. We have been working on this study for a while, and we have heard good things about you. I wanted to mention that before your begin.

You will have 10 minutes to make your presentation. As usual, a question period will follow. The committee members will most likely have some questions for you. I now yield the floor to you.

Ms. Jennifer Stoddart (Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada): Mr. Chair, thank you very much for your invitation to appear again at the very end of your study, which we have been following with interest.

[*English*]

I'm joined today by Chantal Bernier, assistant commissioner, who directs our day-to-day operations, and Barb Bucknell, strategic policy analyst, who is a specialist in social media. They will, I hope, help me answer your questions.

Honourable members, I'd like to start with an overview of privacy challenges.

Over the last few months, I believe you've heard from an array of interested parties on the benefits and the challenges of social media. When I first appeared in May, I noted the four areas of privacy protection where we had the most concern. These were accountability, meaningful consent, limiting use, and retention. It's noteworthy that the witnesses who appeared before you have largely agreed that these areas are challenged by social media. Where they tended to differ, I understand, was on the adequacy of the tools available to address the problems.

Also noteworthy was the extent to which children and youth privacy permeated the discussions. Many interesting ideas were put forth with respect to digital literacy as well as possible legislative responses.

Mr. Chairman, I would like to commend the committee for its insight and forward thinking in holding this particular study.

Today I want to address the key comments that have emerged from your hearings. I will begin with enforcement powers.

The most important question put forward throughout the study was whether PIPEDA is up to the task of handling the challenges brought about by changing technology. Most witnesses felt that PIPEDA needs to be modernized. Others took the position that PIPEDA does not need to be changed, that its enforcement model works, and that its technology-neutral character is its strength.

In my view, with the emergence of Internet giants, the balance intended by the spirit and letter of PIPEDA is at risk. The quasi-monopoly of these multinationals has made PIPEDA's soft approach, based on non-binding recommendations and the threat of reputation loss, largely ineffective, I believe. We have seen organizations ignore our recommendations until the matter goes to court. We have seen large corporations, in the name of consultation with my office, pay lip service to our concerns and then ignore our advice. Moreover, with vast amounts of personal information held by organizations on increasingly complex platforms, the risk of significant breaches and of unexpected, unwanted, or even intrusive uses of that information calls for commensurate safeguards and financial consequences not currently provided for in PIPEDA.

New incentives, including changes to the enforcement model, are required to encourage organizations to be proactive, to build upfront protections, and to ensure secure treatment of individuals' personal information. I agree with the witnesses who stated that PIPEDA's strength is that it is technology-neutral and principles-based. These are characteristics that must remain.

● (1620)

[*Translation*]

I also agree—at least in part—with those who noted my office's success in bringing organizations into better compliance with the law. We have made use of the tools the law provides, and we have been able to effect some change—but often after an arduous effort. That effort comes at high cost to Canadians and is less and less effective against powerful, multinational companies.

You heard the arguments that my office cannot be judge, jury and executioner. In response, I would point you to some of my international and even provincial counterparts.

The United Kingdom commissioner can issue fines, as can a number of the international data protection authorities listed in the document I have submitted today. In the United Kingdom, my counterparts have stronger enforcement powers, but that has not precluded an ombudsman approach. Fines are issued where a softer touch has failed. Our counterparts tell us that businesses that invest in adopting good privacy practices from the start feel it is only fair to impose a financial burden on those who do not, in order to even the playing field.

Commissioners in Quebec, Alberta and British Columbia have order-making powers and jurisdiction over the private sector. They also have other duties—prescribed by law—that enable them to perform multiple roles, such as educator, adjudicator, enforcer, advocate, and so on. I have noted that witnesses before this committee had only good things to say about their relationship with the commissioners. Witnesses have said that the Canadian model was the envy of many countries around the world.

What others like about our law is that it does not single out sectors and is non-prescriptive. Yet, given that many of my international counterparts either have stronger enforcement tools or are requesting them, it is not our enforcement model they are admiring.

Indeed, I worry that, if my counterparts continue to gain stronger powers, but Canada does not, we will fall behind in inspiring consumer confidence needed for the digital economy to thrive.

At the least, we must start with mandatory data breach notifications—including financial consequences for egregious cases. Increasingly, other countries are implementing similar legislation. Such requirements would reinforce accountability and, with penalties, provide financial incentives to better protect Canadians' personal information. Such penalties should be flexible and adaptable to circumstances, so as not to unduly burden smaller organizations.

● (1625)

[*English*]

I'd like now to talk a bit about digital literacy.

Another key theme that has emerged from your hearings is the importance of digital literacy. I believe that the moment has come for government, for educators, and for our communities to seriously focus attention on the digital education of all Canadians of all ages.

Such an effort must address the broader societal and ethical issues that are raised by new information technologies but that fall outside data protection law per se. People need to understand that information on the Internet can live on forever and that they should be careful about what they post about themselves and others. That being said, digital literacy does not absolve companies of their obligations under privacy law.

In conclusion, Mr. Chairman, given the global nature of today's digital economy, Canada's federal law needs enforcement powers comparable to those in other jurisdictions. That is the way to have the greatest impact on privacy protection and to improve Canadians' confidence in their online environment.

A law that dates back to a time before social networks and smart technologies were created cannot remain static. The ways in which personal information in this environment can be collected and used by many players makes a formal study of the effectiveness of our privacy framework even more pressing, so I strongly urge Parliament—and this committee particularly—to move forward with a review of the legislation, PIPEDA in particular.

Thank you very much for inviting me once again, and my colleagues and I would be happy to try to answer your questions.

Merci.

[*Translation*]

The Chair: Thank you very much.

Ms. Borg, you have seven minutes.

Ms. Charmaine Borg: Thank you very much, Mr. Chair.

Ms. Stoddart, thank you for joining us today.

After hearing all the testimony, I'm happy to hear your comments now. Differing opinions have been voiced. We have even heard opinions of international scope. That has really been useful to us.

You recently stated in the media that the Bill C-12 provisions on data breaches did not sufficiently protect Canadians' personal information. You even said that, under those circumstances, you could not fully support this bill.

Could you tell me what amendments should be made to the bill to adequately protect Canadians' personal information?

Ms. Jennifer Stoddart: Thank you for the question.

I officially met with the Deputy Minister of Industry Canada this past spring. I told him that things had changed a great deal since Bill C-12 was introduced in the House—over two years ago, I think. We discussed that, at the time. I said that other countries had implemented legislation and that, in its current form, Bill C-12 was not an adequate solution to the constant and growing threat of data leakage and data-related breaches of confidence. At the very least, we could consider the prescribed threshold, but even more importantly, we should establish a penalty system—even impose fines—which would encourage investments in data protection and would act as a deterrent to breaches of confidence.

Ms. Charmaine Borg: Thank you very much.

A number of witnesses pointed out that you did not have enough power. You also talked about that during your presentation. Even when we went to the United States, people said that the Canadian commissioner was doing excellent work, but that she needed additional powers to successfully fulfill her mandate.

There are many lawsuits against companies like Facebook because that is the only available recourse. If your powers were expanded to allow you to issue orders and impose fines, what would be the best model to follow? We have the examples of Alberta, Quebec and Ontario. Is one model preferable to the others? Do you think one of them works better than the others?

● (1630)

Ms. Jennifer Stoddart: I think it would be preferable for the committee to look at different models. There are various options available, and we have to take into account administrative penalties, fines and the possibility of asking the Federal Court for statutory damages.

In the interest of administrative stability, the least cumbersome model—and therefore the preferable one—is the status quo. Once again, I think the committee should look into this issue. If the need arises or it becomes necessary, the commissioner's office could ask the Federal Court to issue an order. That would not fundamentally change the whole operational model.

Ms. Charmaine Borg: Thank you.

My next question is about the difference between implied and expressed consent. That has been discussed a lot throughout this study.

Do you think it is possible to demand that businesses or social networking companies use a system where expressed consent is required across the board? Is that technically possible and is it advisable?

Ms. Jennifer Stoddart: I will have to ask Ms. Bucknell to answer.

Ms. Charmaine Borg: Okay.

Ms. Jennifer Stoddart: She has spent days, even months, working on this issue. I think that depends on the kinds of matters or contexts where consent is required. This applies in some cases, but not in others.

Ms. Bucknell surely has something to say about that.

[*English*]

Ms. Barbara Bucknell (Strategic Policy Analyst, Legal Services, Policy and Research Branch, Office of the Privacy Commissioner of Canada): *Merci*.

I think it is possible, but organizations need to turn their minds on how best to do it, because there are definitely challenges. Certainly in the mobile environment you have a limitation of space and size, but that doesn't mean it's impossible to tell people very simply and clearly, for example, that this is the information we're going to disclose if you download this application.

Our office has been working hard with our online behavioural advertising guidelines as well as our mobile application guidelines, which we recently released, to reinforce the message that yes, it can be done, and that it should be done in simple, clear language. I think we're going to see more of that from our office.

[*Translation*]

Ms. Charmaine Borg: Thank you very much.

My next question is about policies on privacy and data usage.

We have noted, like you, that companies have been changing their policies over time. Do you think that companies should have to ask for subscribers' consent again? This question is related to the one on expressed consent. Can companies inform users that they have changed their policies and ask whether they want to continue subscribing?

Ms. Jennifer Stoddart: I think that companies should let their members, or their clientele, know that the conditions have changed, since the consent the consumer gave when subscribing did not apply to the new conditions. The company should at least indicate that the rules of the game have changed, so that the consumer can have the option to keep or cancel their subscription.

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

I now yield the floor to Ms. Davidson for seven minutes.

[*English*]

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

Welcome, Commissioner. It's nice to see you back again, and your colleagues with you. We appreciate your appearance here.

It's been a long study, but it's been a good study, I think. We've heard some very interesting comments and we've heard from some very interesting individuals as well as companies. I think that it has been very beneficial and I'm certainly glad we've undertaken this study.

As you pointed out in your remarks, some "witnesses felt that PIPEDA needs to be modernized; others took the position that PIPEDA does not need to be changed, that its enforcement model works and that its technology-neutral character is its strength." I'm just reading that from the comments you made earlier.

We heard from a lot of people on both sides of this issue. We heard about concerns with respect to giving broader powers, including the enforcement powers and the ability to issue penalties, and the concerns that some felt this would alter the good relationship that your office currently enjoys with many companies you examine.

Could you respond to that concern? Do you feel it will affect your ability to deal well with these companies? If you had expanded enforcement powers, how is that going to affect your current relationship in dealings with private companies? You've said in your comments that some people say your office cannot be judge, jury, and executioner. How would that work out? How would the balance be there? Would there be checks in place? In your vision, is that final say in your office?

● (1635)

Ms. Jennifer Stoddart: Thank you, honourable member.

I'm a bit amazed at that statement. It sounds like if we got more power, we would be slinging mud balls at each other. I don't know what hell would break loose if we had enforcement powers.

I had the honour to be the president of a tribunal, one of the ones I mentioned in my speech, that enforced privacy legislation in Quebec, both in the private sector and the public sector. I didn't notice that we had particularly acrimonious relationships with companies in the private sector. I don't notice that my colleagues in British Columbia and Alberta have particularly acrimonious relationships, because they also have an educative role. They also prefer to settle through negotiation, if possible. Nobody really wants to go to court if they can avoid it. They promote the voluntary adhesion to the law.

Therefore I don't see, in those places across Canada where there is some kind of enforcement power, that anybody said the relationships are difficult. If people don't agree and there's one case where you go to the tribunal, well, perhaps people agree to disagree, but I haven't noticed that's prevented my colleagues—or me, when I was in that position myself—from doing educational work, from working with chief privacy officers, from having collegial meetings with the private sector.

I'm a bit perplexed as to that statement.

Mrs. Patricia Davidson: We did hear from many people who felt they had an excellent relationship with your office—I think the majority of people felt that—and they certainly did not want to see it jeopardized.

Could you just talk a little bit more about the comment about judge, jury, and executioner? Those are not always very positive words, but how would you see that happening?

Ms. Jennifer Stoddart: That's another comment that just dumbfounded me. The reality of what we call multifunctional administrative organizations is a concept that is very well known in Canadian law—and, I believe, in British law and arguably in Australian law, to take laws that resemble our public law the most. Both my Australian and U.K. colleagues have different functions: they do education, they do arbitration, they do mediation, they do public outreach, and they also can either impose fines themselves—that's my U.K. colleague—or can go to the court and ask for fines of over $1 million Australian—that's my Australian colleague, so this is a model that's well known internationally.

It's also well known here. Again, my B.C. and Alberta colleagues do education work with us. We've issued several guidance documents together with them. They have a public outreach office and so on, and they are tribunals. They make binding conclusions. Therefore, I don't know why all of a sudden it would be impossible for us, when it has been possible in Alberta, B.C., and Quebec for the last 15 years and it's the rule abroad.

● (1640)

Mrs. Patricia Davidson: Do those other jurisdictions have any arbitration process?

Ms. Jennifer Stoddart: I'm not sure—

Mrs. Patricia Davidson: An appeal process, I should say.

Ms. Jennifer Stoddart: There is an appeal process, yes. In the case of Quebec, there's a direct appeal. I believe in the case of Alberta and B.C. there's judicial review, which to me is usually a higher standard.

Mrs. Patricia Davidson: In your remarks you also talked about digital literacy. We've heard a fair amount about that from a very broad range of presenters during this study.

We heard about it when we talked about children, for example, but we also heard about it for adults as well. There is an age group that is fairly well educated about social media. There's an age group that isn't educated well at all. Then we have young kids coming up, learning at a very young age.

When you talk about digital literacy, how do you see that happening? Who do you see being responsible for it? Is it a shared responsibility? Is it something your office would become more involved in down the road?

Ms. Jennifer Stoddart: Yes.

I would think there are any number of players across Canada, both federally and provincially, in digital literacy issues, depending on whether you're addressing it to school children, parents, young adults, or seniors, who kind of skipped that altogether.

We're involved to the extent of our resources, and we just launched, with the Media Awareness Network, a tool about mobile app guidance for educators in school boards across the country.

There are any number of players. That activity could be developed, but we wanted to bring this tool to your attention.

[*Translation*]

The Chair: Thank you, Ms. Davidson. Your time is up.

I now yield the floor to Mr. Andrews.

[*English*]

Mr. Scott Andrews: Thank you.

Welcome, folks. It's a pleasure to have you here again.

I always ask a question to witnesses during this testimony about where they raise their privacy bars. Most of all I think these companies, which are basically in the United States, are scared of the FTC. That's the primary privacy body that they listen to. With anything else, I think they're just paying lip service. Is that a fair statement?

Have you seen that these companies, when dealing with your office or other offices in other countries, actually do take some of these things and raise the privacy bar to the highest standard, or are they just taking whatever the FTC says as the minimum, and that's all they're going to do?

Ms. Jennifer Stoddart: Certainly American companies, which are the major players on the Internet, have the FTC's opinion in their sights.

Could I ask assistant commissioner Chantal Bernier, who directs our day-to-day investigations, to give you a recent example of the truth, I think, of the statement you put forward about the FTC and other privacy commissioners?

Ms. Chantal Bernier (Assistant Privacy Commissioner, Office of the Privacy Commissioner of Canada): Thank you, Commissioner.

Yes. I think this story is quite eloquent.

You may recall, if you have followed the press clippings around our work, that in 2011 we issued a report of findings on Google WiFi. We found that as Google was rolling out Street View, they captured—accidentally, they say, and we have no evidence otherwise—personal information of Canadians. We gave them one year, a full year, to present to us a third party audit assuring us that they had applied all the recommendations we had made.

That timeline was May 20. At the beginning of May we had a meeting with Google, and our request for a third party audit, which was clearly stated in our letter, did not even seem to be on their radar screen. They were rather apologetic, and said "Oh, my God, can we have an extension?" In July, they sent us the third party audit that in fact had been written for the FTC.

I believe that truly goes to your point.

● (1645)

Mr. Scott Andrews: Another question I had about recommendations was how we make this apply. How do we make these companies apply the Canadian standard, or your office? Is the only way to make them apply it to bring them to court and put a penalty on it?

How do we make this happen? How do we make them apply our privacy standard?

Ms. Jennifer Stoddart: Well, from observation over the years, I think it is the only thing that makes them sit up and take notice.

Their names are already public. We're dealing with a far different breed of companies from what existed when PIPEDA was adopted. Lawyers have said to me many times over the years, "I wish there were more sanctions", or, when I started talking about sanctions, they say they are so happy we are doing that because their client—this could be an outside client at a law firm or the CEO of a company where they are an in-house lawyer—asks them to draw up all the regulatory risks and then asks, "What happens if I don't?"

When they get to privacy, they ask what happens if they fall off the Canadian privacy wagon. Well, I have to say, "Don't worry. There will be an investigation, and in the course of the investigation, you can promise to fix it", and that's it. That's what the law says. If they promise to fix it and there's an agreement, I don't take them to Federal Court, so they say, "Okay, fine; put it at the bottom of the list."

As a result, the lawyers who were advising their clients can't get their clients to pay attention to Canadian privacy law because the CEO asks, "What are my biggest risks?" If there's virtually no risk of infringing when you infringe a Canadian privacy law, you move on to other things. That includes data breach, as we were talking about earlier.

Mr. Scott Andrews: I will get back to the data breach, because that was the minimum request. If we do put in a penalty, if we do put this into Canadian law, how can the courts enforce this? How can the courts put a penalty on it, if most of their work is in the United States?

How does this cross borders? How we are going to be able to make them pay if they don't live up to our standard?

Ms. Jennifer Stoddart: I think it's been done already by the Federal Court. I think there's a legal test, a real and substantial connection to Canada. I think many of the companies meet it. It's fairly clear, and that test would have to be met.

We would be levying a sanction for their behaviour involving the personal information of Canadians. I don't think there is a problem of enforcing it. Other countries enforce things against companies headquartered elsewhere. It depends on how your laws are written, but one of the many good things about PIPEDA—the only thing I'm raising here is the lack of enforcement powers—is that PIPEDA is written in a such a neutral way that as long as you have a connection with Canada, it doesn't matter where you are headquartered. It doesn't matter where your servers are, etc. I think that can be dealt with in a rewrite of the law.

Mr. Scott Andrews: Have you thought of what range of fines would be appropriate for us?

Ms. Jennifer Stoddart: Yes. I would think it would be interesting if you looked at the range of fines the European Union is currently contemplating. There's a range of fines; first tier, second tier, third tier. It goes up to a maximum of 2% of worldwide revenue. There's debate about that and so on, but if you look at the fines the FTC is imposing, a range of $20 million to 25 million....

Mr. Scott Andrews: The FTC model is interesting because it's not really privacy, it's—

Ms. Jennifer Stoddart: Yes, well—

Mr. Scott Andrews: —their back way of doing it, and—

Ms. Jennifer Stoddart: Exactly—

Mr. Scott Andrews: —they acknowledge that.

Ms. Jennifer Stoddart: Exactly.

Mr. Scott Andrews: If you stay off their radar.... I found that a bit bizarre, but I guess that is just their system.

Is that only for mandatory breach notification? Let's drill in, because you said we should start with that at a minimum. What levels should there be? What would be the maximum?

● (1650)

Ms. Jennifer Stoddart: I think the maximum that the European Union.... I remind you that PIPEDA was adopted so that we would meet European Union standards, and 80 countries in the world have now adopted the European model.

From memory, there are maybe 15 countries outside the European Union that explicitly meet the European standard. Canada was the first one. We should continue to look at the European model and have these different levels of fines that start at perhaps a few thousand euros and go up to something major. That's because you may be dealing with a small, local family business that just doesn't want to pay attention, or you may be dealing with a big multinational player.

[*Translation*]

The Chair: Thank you, Mr. Andrews. You're out of time.

I now give the floor to Mr. Mayes.

[*English*]

Mr. Colin Mayes (Okanagan—Shuswap, CPC): Thank you, Mr. Chair.

Ladies, thank you for being here today.

I have to say that this study has enlightened me about what goes on in social media and some of the challenges you have.

In your statement, you discussed four issues, which were retention, meaningful consent, limiting of use, and accountability.

To me, retention, meaningful consent, and limiting of use are very simple to deal with through laws or guidelines for compliance. You have to spell out what that should be. What I understand from the witnesses is that simplicity is important for the user. Accountability is really the issue, I think, and your biggest challenge.

To make those providers accountable, would you regulate on a complaint basis or a monitoring basis?

Ms. Jennifer Stoddart: In speaking of accountability, which is one of the features of the Canadian law that has become very popular internationally because it well encapsulates the obligations of companies to privacy law, I think ideally—and this is why I would urge the committee and the honourable members to think of embarking on the second review PIPEDA that is already overdue—that it would be very helpful to have in the law that the Office of the Privacy Commissioner could request companies to show, to demonstrate, how they are accountable. We have an entire document on that, honourable member, that we could send to you.

It basically means being able to demonstrate that you have done all the things to make sure that you are privacy compliant: that you have a chief privacy officer, that your staff has been trained, that they know what to do, that you don't retain data longer than necessary, that you've invested in securing personal information, that you have the right procedures so that when people come under the law asking to see their personal information, you know how to handle that, and so on. Accountability goes to the range of your obligations under the law.

Presently when we go in for an audit or go in because of a complaint, we look at how the companies have been accountable, but we don't have a specific proviso that says they must show us how they are accountable.

Mr. Colin Mayes: The previous witness said something that was quite interesting to me. He said that the platform is anonymous, so it really isn't an issue of the privacy of the person. It is the privacy of the site that they use to access their platform.

This puts in my mind what are we protecting here. Is the culture of privacy? Modesty and several aspects of what I consider private are different today from what they were 10 or 20 years ago. Is that fence post moving? On what do you base what you would call your scope of privacy or your principles of privacy?

Ms. Jennifer Stoddart: As to the first question, honourable member, I didn't hear that. I don't quite understand what that gentleman meant. Perhaps we could go back and look at the transcript, and I could give you an answer on that.

Mr. Colin Mayes: Maybe I could just take some time to explain. Maybe Mr. Calkins could help me here, because he's very knowledgeable about this aspect. He said that when they're gathering information, they're gathering information about the site, not the person. The person might be sharing information by looking for a new vehicle or something; that information is stored and marketed so that those who are selling vehicles can set that cookie in place, but the actual personal information—what I call personal information—is not necessarily shared. It's what the site activity is; it's what's happening on that site, rather than the person's personal information.

● (1655)

Ms. Jennifer Stoddart: Right. Yes.

Mr. Colin Mayes: Can you differentiate between those two, and then also—

Ms. Jennifer Stoddart: The culture of privacy.

Mr. Colin Mayes: —the culture of privacy.

Ms. Jennifer Stoddart: On that I would say, yes, that's what we hear often—that they just want to see what site you visit—but from our own work on what you can find out by tracking, the problem is that you can aggregate all the sites that I have visited and then draw up a profile. In some cases you could find my name and my address from public sources, and so on, and you could draw up a profile of me as a citizen or consumer that can be accurate or it can be extremely inaccurate.

As the Internet becomes more sophisticated.... There's an article by the American scholar Jeffrey Rosen that's very good on this. It was published about two weeks ago.

The danger of tracking and the issue of discrimination on the Internet is that because you have visited these sites, the ad server can decide that you fall into a certain category. We can't each have a personally individualized category for the moment, but we'll say "middle-aged lady, likes golf, likes to drive station wagons". In the American example, because of different political sites that were visited, it could be "votes this way, thinks this way", and so on. It can be accurate, but it can be inaccurate.

The fact that it will determine the information you get, the ads you get, and sometimes, I believe, the rankings in search engines—I'm not sure about that—means that your experience of the Internet and the world of knowledge that the Internet represents will be limited. It will be based on what may be a true or a false or a partly true profile that algorithms are determining for you.

That's some of the concern: that you fall into artificial categories and therefore only see the information that is deemed to fit in with the artificial category into which you have fallen.

Mr. Colin Mayes: The other question was on the principles of what you consider privacy.

Ms. Jennifer Stoddart: That's a hugely broad question, and the issue of privacy goes well beyond my mandate. I only have a mandate for personal information handled either by the government or by organizations.

In PIPEDA, for example, we enforce the Canadian Standards Association's code, which is an appendix to PIPEDA, and that's based on OECD work of the early eighties.

Mr. Colin Mayes: Thank you.

[*Translation*]

The Chair: Thank you, Mr. Mayes. Your time is up.

I now yield the floor to Mr. Angus for five minutes.

[*English*]

Mr. Charlie Angus: Thank you. It's great that you came back.

Our first witness said something interesting. He spoke about self-regulation and some of the industry players we have. They have standards. Other people don't have standards. He said self-regulation worked very well as long as you had an enforcement mechanism.

I sometimes think my colleagues on the other side hear self-regulation as the market mantra. If that were the case, Somalia would be a centre of international innovation—but it's not, because they don't have the enforcement mechanisms to decide what is good activity and what is bad activity.

In our case it comes down to breach notification. That's one of the key bottom lines, I think. If my data is breached, it's not just what site I go to or what I'm interested in or where I play golf, but the fact that I use my credit card to buy stuff. If that data is breached, my security is at risk.

Under the rewrite that's being planned by this government, their language is interesting. They say it has to be a "real risk"—not a perceived risk, but a real risk—"of significant harm". If I were a corporate lawyer, I'd say I wouldn't tell anybody that their data has been breached. Significant risk means what? Nobody's going to come and kill you.

It seems that the government is setting a bar so high that the companies have an opt-out mechanism and are not going to report breaches even if it's credit card information or personal data information, something that the cyber hackers would love. Do you think we need to clarify at what point a company has to inform you that the cyber hackers have been visiting your data?

Ms. Jennifer Stoddart: I think, honourable member, we have to revisit this question, and that's why I spoke to the Deputy Minister of Industry. I think that the draft legislation was drawn up maybe two or three years ago with what we knew then. I think we have to go back now and look at some of the laws, at how they function, what we know about adverse effect on consumers, and so on. The question has been raised of whether this is too high a bar, given the frequency of data breaches, and I think that question should not only be asked again, but studied and answered.

● (1700)

Mr. Charlie Angus: In terms of allowing the market to maintain itself here, we have an extremely high bar that has to be met, and a lot of stuff can slip under it with no enforcement mechanisms. From your comments I'm seeing that we are going to fall behind all the other western countries when it comes to having those enforcement mechanisms.

I don't know if the comparison is correct, but in the copyright wars we heard all about Canada being a Pirate Bay because we didn't have enforcement mechanisms. I think some of the language was a little over the top, but if data breaches occur in the market we have, people don't have to worry about it because nobody's coming after them, and if they do come after you, if you're beyond shame, what are they going to do?

Perhaps certain companies would prefer to set up and do business here in Canada. They'll say they're under Canadian law and they shouldn't be bothered. They'll set up here because they'd get hammered in England, hammered in the EU, and hammered in the United States.

Because we have always been the world leader, should we not establish a similar standard that matches where the other main western countries are?

Ms. Jennifer Stoddart: I would think so, and I continue to be concerned that we don't have any data breach legislation at the present time, except in the province of Alberta.

Mr. Charlie Angus: Second, it seems an odd situation to have data breach provisions in certain provincial jurisdictions and not in others. With this whole balkanization of our privacy regulations, someone just has to look for the easiest point to go to in Canada and set up there. Is that the kind of innovation standard we want to have? If you want to be a cyber hacker you come here, but if you want to do good innovation and be a respected company.... In Europe and the United States, you know that if you play by the rules, you're going to be looked after, and the companies that don't play by the rules are going to get nailed.

Isn't it important to have a cross-Canada standard, as opposed to various provincial systems?

Ms. Jennifer Stoddart: Well, I can't speak to the provinces, which do what's in their jurisdiction, but as federal Privacy Commissioner I'm particularly concerned that the federal government jurisdiction over such entities as banks, for example, has no specific data breach provisions. We know that banks are a particular target for data hackers.

[*Translation*]

The Chair: Thank you, Mr. Angus. Unfortunately, you're out of time.

I now yield the floor to Mr. Calkins for five minutes.

[*English*]

Mr. Blaine Calkins: Thank you.

I just have one question. Then I'll pass my time on to one of my colleagues.

It's the question about being able to provide an administrative penalty, Madam Commissioner. You've often referred to the European model, which has a scale based on the size of the company in question and so on.

What could you do and what would be considered fair, outside the judicial system's practice of due process before the law? In the event of a material breach of an individual's privacy, whether a data breach at a banking institution or whatever the case might be, what size of penalty do you think you would need in order to appropriately levy a fine to provide a deterrent or an adequate punishment for a company such as Google or Facebook or some such, which are multi-billion-dollar companies?

Ms. Jennifer Stoddart: Thank you for the question.

I haven't looked at the size of data breach fines, which are for something different from simply not obeying the law on consent when sharing personal information.

My remarks on the size of the EU fines were that they relate to whether you respect the law or generally do not, whether there was a data breach, and whether it happened because basically you weren't investing in security. We've seen that time and time again.

I believe that Industry Canada, which drew up the legislation, is best placed to look at what would be appropriate fines. My only point here—and I didn't come here prepared to talk about it, but the question was raised—is that we need some kind of appropriate sanction. How big that is, I can't answer, but I don't think we should go ahead with that part of Bill C-12 at this point, if Bill C-12 lags so far behind the world standard.

● (1705)

[*Translation*]

The Chair: Mr. Dreeshen, you may continue.

[*English*]

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

I have just a couple of comments, as I've had a chance to talk to different businesses that have been involved in this area.

One of the concerns I have when you set the bar relatively high—and I think you went through a list, saying that each company should have various levels of individuals who can ensure that you have the privacy that you require—is whether we then start to be concerned about picking winners and losers. Perhaps the bigger companies, which already have that mechanism, are able to expand, and the smaller businesses then know that they have all of this level of privacy legislation and so on that they have to get to.

I'm concerned about that, with the small businesses coming in. That was one thing we heard right off the bat: that if you put the rules in right away and make them too stringent, the only ones who are going to be successful are the ones who are big enough to take on the burden that is being presented to them. That's not how you gain innovation.

When you take a look at some of your suggestions—as no doubt you will, when you think about what we have been studying—I wonder whether you could look at the question through that particular lens, because we want to make sure we're not stifling innovation. That's the first feeling and thought that I have with regard to this issue.

The other thing we've tried to talk about to people who have come here is that it isn't free. When we suggest that if we get on the BlackBerry and do this, that, and the other thing, we all of a sudden have the free range to do whatever we want and we're going to be protected from ourselves, based on some of the activities that we have.... I look at it from that perspective.

If you go into a store and take a magazine off the shelf and start reading it there, somewhere along the line you have to go and buy the thing; you have to recognize that this is part of what we do. I haven't really heard a lot of discussion from regulators that really recognizes this. When you ask businesses about how they make their money and what they do, you get a bit of an understanding of where you're going with that.

If I have a few seconds, my last comment is about the right to be forgotten. One of the analogies we heard was of someone taking a glass of water and pouring it into a stream; it goes all the way through, and at the end of days they say, "I want my glass of water back" after it has gone through the river and down into the ocean and so on.

There are different thoughts on this aspect. I wonder whether you could comment on some of my ramblings there in the time I have remaining.

Ms. Jennifer Stoddart: I understand, honourable member—

[*Translation*]

The Chair: I apologize for interrupting you. The time is up, but I will give you about a minute to answer.

Ms. Jennifer Stoddart: Did you say three minutes?

The Chair: I am giving you about one minute.

[*English*]

Ms. Jennifer Stoddart: Okay.

Very quickly, then, in one minute: first, we have always tried to tailor the law to small and medium business. Some of the examples I'm talking about here are mega-megacorporations, not small and medium-sized businesses.

Second, on stifling innovation, I don't believe innovation always has a direct link to privacy. I think innovation is mostly encouraged by capital formation, entrepreneurial capital that's free, and levels of education or technical knowledge.

Third, my office has no objection if people want to sell their personal information to get services free. We have never said that. We have no problem with the Internet model. We just want the law that Parliament adopted in 1999 to be applied correctly: you have to consent, and you have to understand what you're selling and what will be done with it.

Fourth, on the right to be forgotten, I think this right is an important concept. We have to seriously look at the ways and means of enforcing it. Parliament in its wisdom said that PIPEDA that you have a right of deletion of your personal information, so we in a sense already have it, but we have big issues with some companies who built in no ability to delete young people's information.

[*Translation*]

The Chair: Thank you for your answer.

I yield the floor to Mr. Boulerice, who has five minutes.

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

Madam Commissioner, ladies, thank you for joining us.

As my colleague was saying, it's useful to hear from you at the beginning and at the end of the process. I will take a few seconds to say that this study, thanks to my colleague, has been something of a revelation for me. It has opened my eyes to the fact that we are monitored much more than we think on the Internet and in social media. I didn't know how much we were being monitored and watched.

I feel that this is the case for many Canadians who accept the conditions quickly and then go on to browse various websites. They are unaware of the machine behind it all—be it browsers, Google, social media or these data brokers, which I didn't even know existed not too long ago. They gather a great deal of information about us—our habits, choices, preferences, places we visit, purchases, ideas. Afterwards, they put all that together and often sell the information. I think that, according to what you have told us, the role of educator—which you should play more—is as important as the power to impose fines or penalties.

Could you tell me what you think of Canadians' digital knowledge or digital literacy? Do people know that they are being monitored so much?

● (1710)

Ms. Jennifer Stoddart: We conduct annual surveys. One year, it's a survey of companies, the next year, it's a survey of citizens. Canadians are very concerned about their privacy; they think this is one of the major issues of the future. Unless I am mistaken, 40% of the people we have surveyed identify Internet as a possible source of privacy violations. In general, people are uncomfortable with explicit monitoring by video cameras or monitoring on the Web, but they are not very informed because the matter is complicated to understand.

Mr. Alexandre Boulerice: You said that the bill introduced in the House is now two or three years old, but that it has not been passed. Perhaps a comprehensive review is necessary, where certain provisions would be amended because the digital world and the Internet have changed since then. You told us that inaction is risky and that, if nothing is done, we will fall behind other western countries. I would like to know what you think is the potential consequence of our inactivity regarding the protection of Canadians' privacy. What kind of an impact will that have on people?

Ms. Jennifer Stoddart: I think it's unacceptable that, in 2012, Canada does not have any legislative protection against data leakage —with the exception of Alberta. About once a week, companies or the government itself voluntarily report to our office leakages that affect thousands of citizens and consumers.

In the United States, 49 of the 51 states apply legislative protection or deterrent measures. That approach does not only consist in deterring companies. Businesses are also required to provide a free assessment of the credit rating. One year later, they have to check whether people are affected by the data leakage and, if so, undo the resulting damage.

I think the fact that Canadians are not provided with this protection is a serious matter, and I hope that the government will introduce relevant legislation very soon.

Mr. Alexandre Boulerice: Especially in the banking sector, where everyone would like to see things more tightly regulated, for obvious reasons.

Ms. Jennifer Stoddart: Exactly.

Mr. Alexandre Boulerice: Do I have a little time left?

The Chair: You have 30 seconds.

Mr. Alexandre Boulerice: You are very generous, Mr. Chair.

Do you feel that self-regulation on the Internet and in social media is enough? In discussing previous testimony, we talked about harmonizing the voluntary rules. But when we talk to people from the industry, we get the impression that no adequate oversight mechanism is in the works.

Is it enough to let people get together to decide the way in which they will operate, with no one overseeing them?

● (1715)

Ms. Jennifer Stoddart: No, I don't think so. That approach does not work. In the United States, the entire advertising industry has been talking about it for several years. They have never managed to come to an agreement on self-regulation. Self-regulation is fine, but I feel that it needs legislation to back it up. As the Americans have not been able to make it work, it is possible that they will come up with legislation.

Mr. Alexandre Boulerice: Thank you.

The Chair: Thank you, Mr. Boulerice.

My thanks to the commissioner for coming to testify before us today. For all practical purposes, that is the end of the testimony for this study.

Now we are going to break for a few minutes to talk about the future business of the committee.

Ms. Jennifer Stoddart: Thank you.

The Chair: As you know, we are going to have to find something to do when we get back after the holidays.

Ms. Jennifer Stoddart: Thank you very much, Mr. Chair.

My thanks also to the members of the committee.

[*English*]

Thank you very much for being so interested in this issue. It is, I think, the most important parliamentary inquiry into privacy matters that we've seen for a long time. I'd just like to say how much our office appreciates your work.

Thank you. *Merci*.

● (1715)

(Pause)

● (1715)

[*Translation*]

The Chair: Order, please.

Now we are going to deal with future business of the committee. Mr. Warkentin, you have the floor.

[*English*]

Mr. Chris Warkentin (Peace River, CPC): May I make a motion to move in camera? There are a number of things that I think we'd all like to discuss, but it's regarding future business and it would be, I think, more effective if we did that in camera.

[*Translation*]

The Chair: We have a motion to continue the session in camera and a recorded vote has been requested. I will let the clerk conduct the vote.

(Motion agreed to: yeas 9; nays 2)

[*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