



HOUSE OF COMMONS  
CHAMBRE DES COMMUNES  
CANADA

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

---

ETHI • NUMBER 058 • 1st SESSION • 41st PARLIAMENT

---

**EVIDENCE**

**Thursday, December 6, 2012**

—  
**Chair**

**Mr. Pierre-Luc Dusseault**



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

Thursday, December 6, 2012

• (1535)

[Translation]

**The Chair (Mr. Pierre-Luc Dusseault (Sherbrooke, NDP)):** Welcome to this 58th meeting. We will continue our study on social media and privacy.

During the first hour, we are very lucky to have Ms. Pirri, who is the legal counsel for Twitter. During our second hour, we will hear from a representative of Acxiom via videoconference.

We will begin with a 10-minute presentation, followed by questions.

Ms. Pirri, you have the floor.

[English]

**Ms. Laura Pirri (Legal Counsel, Twitter Inc.):** Thank you very much, Mr. Chairman. Thank you, other distinguished members of the committee. It is a great pleasure to be here in Ottawa with you today to discuss the important subject of social media and protection of our users' personal information.

As some of you know, Twitter is a global communications service that was created in 2006. Since its inception, Twitter has been designed primarily to enable users to share information publicly with the world. In the short span of our company's history we've seen how Twitter can bring people closer and help them feel more connected to what's going on in the world. Twitter can be a very empowering tool for users to be global publishers and information consumers.

We've been privileged to be a platform for famous artists, such as Ai Weiwei, who, although he cannot leave China, can communicate with the world via Twitter.

Twitter has also been used as a platform for the Royal Canadian Mounted Police. They've used it effectively for community outreach, for recruitment, and for offering support to gays and lesbians who were victims of abuse and bullying.

We are very proud of the role Twitter plays in giving voice to the stories of millions of people every day.

Let me give a little context about how Twitter works. As some of you know, Twitter is a free service that allows people to publish and receive short messages, 140-character messages called "tweets". Most people using Twitter have accounts. You sign up for an account, and you're able to follow other users. You can automatically see their tweets in your timeline, which is the stream of tweets that you see when you log into the service—although you do not need to have an account to use Twitter to see publicly visible tweets.

Because of the ease of following on Twitter, the ease of using the service as a publishing platform, we now have more than 140 million users around the world. They publish more than 400 million tweets per day in many different languages. There's a real diversity of users and interests represented on Twitter.

We've seen it used for politics and news, art, music, entertainment, sports, fashion, food, culture—you name it. We've seen politicians engaging with citizens. We've seen celebrities responding to fans. We've seen individuals seeking and obtaining redress from global companies. We've seen online literature, charitable campaigns. We've even seen calamity and natural disaster. It's been a way that we could witness what's going on in other parts of the world.

Our goal is to be the platform for the global public conversation, for the global town square that Twitter has become.

Let me talk a little bit about our approach and commitment to privacy, but let me tell you first a little bit about who I am. As you know, I'm Laura Pirri. I am one of the legal counsel at Twitter. My primary responsibility is to advise the company on some of its product initiatives. That includes data protection issues, and it includes compliance with our privacy policy.

Privacy, though, is something the lawyers in the company... We aren't the only ones who think about it. We have a set of company values, and one of our company values is to defend and respect the user's voice, and that includes respect for the user's personal information.

Our service doesn't require a whole lot of personal information in order to use it. As I mentioned, you can use the service without actually having an account. If you have an account, you don't need to provide a real name or a street address. You don't need to provide age. You don't need to provide gender.

• (1540)

Also, you can protect your tweets if you don't want them to be publicly visible, although it's worth noting that most people come to Twitter in order to share information publicly. They want their tweets to be public.

Drawing on our company values, when we're launching and designing our product features, we do so with privacy in mind. For example, one of our privacy philosophies is to provide contextual notices or disclosures to users in the product at the time that they provide us with information, in order to supplement our privacy policies. I did actually listen to some of the questions that you asked previously.

One of the questions you asked was about privacy policies: do users read them and how do we know that users are aware of our privacy practices? One thing to help ensure that users are aware is to provide additional disclosures, to provide these kinds of contextual notices. Let me give you an example of how we do that. It's our "tweet with location" feature. Since I know that some of you are active users, you may know how this works, but we have a number of different notices and controls around the tweeting with location feature.

First, in order to tweet with location, you have to actually turn it on in the settings. You go to the account settings and you turn on the "ability to share location with Twitter". Once you've turned it on, when you go to the tweet box, you'll see a location icon that's in the area where you compose your tweet. You have the option to turn location on or off on a per-tweet basis, so you can decide with each tweet whether you want to include your location in the tweet. There's also information about tweeting with location, how it works, and what it means. In addition, if you've tweeted with your location, you can also change your mind later and decide that, actually, you don't want your location in those tweets, so you can go to your account settings and remove location from your tweets without actually deleting the tweet itself.

Twitter is still a young company. It's certainly younger than the other companies you've had here. We're keenly aware that our platform must serve our users well and that we must earn their trust by providing a robust service that is engaging and also safe and secure. Let me close with an example of how we work hard at achieving that balance. I want to talk about a product launch we had earlier this year that I was involved in.

We launched a product feature to tailor suggestions for users, suggestions for accounts to follow in the service. We wanted to help them find in the service more accounts that they might be interested in. For those of you who use the service, I'm sure you know that Twitter is better when you're following people who are talking about things that you're interested in at the moment.

What we found was that we could make much better suggestions for users to help them follow accounts that they're interested in, based on the accounts that are frequently followed by other users who visit the same websites in the Twitter ecosystem. The Twitter ecosystem is all the other websites that have integrated Twitter's buttons and widgets, like our "tweet" buttons and our "follow" buttons that allow you to tweet from other websites or to follow users from other websites. We found that this was a really great way to present users with current and interesting suggestions for who to follow on Twitter.

I'm sure, as many of you know, that this is not unique to Twitter. Other services that are integrated into websites—LinkedIn, Facebook, or YouTube—also receive this kind of web visit information when users visit pages in which their services have been integrated.

We're very excited that we could make much better suggestions for users to more quickly and easily find what they're looking to follow on Twitter. At the same time, we really wanted to give users simple and meaningful choices around the collection of this information and whether it's collected and used for improving their service experience.

● (1545)

We are very proud to be one of the first major Internet services to implement "do not track". We implemented it as a way for users to let us know, by setting "do not track" in their browser, that they do not want this information collected. That way we can improve their service experience by making better recommendations. I think it's important to stress that this is a "do not collect" implementation that we made, because we actually don't collect the information. There's been a lot of discussion around "do not track" and exactly how it should be implemented.

We worked collaboratively with the United States Federal Trade Commission in our "do not track" implementation. We also worked with a lot of lawmakers and advocates in the privacy community in the United States, and we were really thrilled with the praise they gave us on our implementation. It was an honour, and we were very appreciative of the kind words they had.

Although we do not have an office here in Canada, and we don't have employees here—in fact, today is our first visit as Twitter employees to Canada—we did reach out to the Office of the Privacy Commissioner here in Canada at the time we did this product launch just to let her know what our plans were and that we planned to implement this product feature and support "do not track". We hope that our support of "do not track" shows its value as a consumer tool for privacy, and we hope it encourages wider adoption of it as a privacy preference for users.

Thank you very much.

[*Translation*]

**The Chair:** I forgot to mention at the beginning of the meeting that we thank you for being here. This is very much appreciated, all the more so because of the fairly short notice. I hope that you don't find it too cold in Canada.

So without further ado, I will give the floor to Mr. Angus for seven minutes.

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

[*English*]

Thank you very much for coming. We're very pleased that you're here, because we're in the final stages of this study. I think that as legislators we're looking across party lines, though I can't speak for my colleagues over there, and I never would try to. We don't want reactive legislation. We want legislation that works so that we can allow the platforms to develop. To us, at least those of us in the New Democratic Party, the enormous possibility for democratic engagement is an essential element.

We think we have a strong privacy regime in Canada. We believe Canadians really value their privacy. They are crazy users of social media—they're all over—but they still want that balance. The question is, how do we strike that balance?

I'd like to ask you about some of the experience with Twitter, because its set-up is different from, say, Facebook's, so it has different strengths and weaknesses. Because of the anonymity features, we've seen a number of cases recently of threatened lawsuits, such as that of Lord McAlpine, who threatened 10,000 Twitter users with lawsuits over re-tweeting allegations about him.

This is certainly putting us into new territory in terms of what is libel and where libel applies. When someone says they're going to sue 10,000 people, 9,000 of them for re-tweeting something that damaged someone's reputation, how does Twitter work with that? Do you say you have to bring a production order to get the data on these anonymous names? Some of them might be obvious, but the vast majority will have an anonymous handle, so how does Twitter deal with those kinds of situations?

**Ms. Laura Pirri:** We post the law-enforcement guidelines and we require that if you're seeking non-public—so, private, personal—information about our Twitter users, you provide us appropriate legal process, so a subpoena or court order. This is in the interests of protecting our users' privacy.

We also are committed to transparency around law-enforcement requests, so we always notify users when someone has requested their information in this way. This would be the process we would ask parties to pursue if they were looking to receive information.

• (1550)

**Mr. Charlie Angus:** It would seem to me somewhat difficult to launch 10,000 lawsuits unless you had endless amounts of money. In Lord McAlpine's case, I think he was asking for apologies from the tweeters.

In that case, would you insist on production orders for each of the 10,000 against whom a case was being brought? Do you deal with his legal team? It will be somewhat precedent-setting if this kind of case goes forward.

**Ms. Laura Pirri:** I'm not familiar with the specifics of his case.

I think Twitter, similar to the Internet, is a platform for speaking. The dispute resolution aspect of identifying the speaker you're talking to certainly has its challenges. I'm not sure Twitter has a role. We have rules that govern the use of our platform, so of course, we expect that the people using our service are in compliance with our rules. If it's speech that's otherwise in compliance and not unlawful, the users are going to have to find ways to resolve their disputes. Unfortunately, if it goes into the court system, this is a challenge in bringing litigation.

**Mr. Charlie Angus:** I'll give you a different example that came to our committee. A staffer in the Liberal Party set up an anonymous Twitter account and released the court affidavits of a cabinet minister's very messy divorce. I don't think anything in it was inaccurate, but it certainly caused a brouhaha. The staffer killed that account. Now, what happens to that information? Is it still part of the Twitter database?

**Ms. Laura Pirri:** You're saying that someone deleted the account.

**Mr. Charlie Angus:** Someone set up an account, released all kinds of gory details about a very messy public divorce into the Twittersphere, then got political heat, and then shut down the account. There's nothing actionable, as far we can see. Where is that

data? Does it disappear when the person shuts down the account, or is that part of the Twitter database?

**Ms. Laura Pirri:** Again, I'm not familiar with the specific situation. A user can deactivate an account. It's in your account settings. We have a process for account deletion to happen soon after. There's a 30-day grace period during which your account is deactivated. It's removed from the service as of the time you deactivate it. Then it's deleted. The process for deleting starts happening 30 days later.

**Mr. Charlie Angus:** You're dealing with a reseller, Gnip, to launch the historical power tracker for Twitter, which provides access to the complete data archives. It says that there are 30 billion social data activities a month being delivered. I guess that would be the history of people's tweets. Does that include deleted accounts, or do deleted accounts become deleted information?

**Ms. Laura Pirri:** For parties accessing public information through our public APIs, when tweets are deleted, they are deleted from the public API stream as well.

**Mr. Charlie Angus:** I notice that there's Politwoops. It's about politicians who delete their tweets. I have to say, having followed some of my colleagues, that sometimes when they really mean to say things, they are pretty inane, so when they have to delete something, it's usually really idiotic. It's usually after nine o'clock at night on a Friday night and they panic and realize, "Oh my God, did I just do that?" Then they press the delete button, which seems to kick off an algorithm at Politwoops. They grab it and put it on the site so you can check infamous political tweets that were deleted.

Does that happen with Twitter? Does the embarrassing tweet get deleted from Twitter when it happens, and does Politwoops pick it up from the ether? How does that work?

**Ms. Laura Pirri:** I'm not familiar with Politwoops.

**Mr. Charlie Angus:** It's fascinating. It's actually the best Twitter feed I've read recently, and I don't even read Twitter anymore.

A politician deletes something he or she said that is absolutely inane, because the person drank two bottles of wine and wanted to pick a fight with another politician. Does it disappear, or does it become...?

**A Voice:** It would never happen.

**Mr. Charlie Angus:** It would never happen on our side. I'm looking at some of my colleagues, but not the ones in this room, of course.

What would happen to the tweet? Does it disappear into the netherworld, or is it there as a permanent record?

• (1555)

**Ms. Laura Pirri:** We wouldn't be providing it through our API. Now, if people already have it in their possession prior to deletion, it sits there. They copied it. We can indicate that there's a deletion notice. People who are using our APIs under our developer terms are required to honour these deletion notices. It sounds like they're letting them remain on.

**Mr. Charlie Angus:** I just want to be on the record that I'm not saying we need digital mittens to protect politicians from being stupid. I was just wondering what happens if they delete the tweet, if it disappears.

[Translation]

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

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

**The Chair:** I will now give the floor to Mr. Butt for seven minutes.

[English]

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

Thank you, Ms. Pirri, for being here. Welcome to Canada. We're glad to have you here for those of us who are rabid tweeters, not as rabid as Kady O'Malley is in the back there, but some of us like to send lots of tweets out. We even have our friends like Mr. Angus, who used to do it and then decided to quit.

I didn't know about this Politwoops thing so I think that's kind of interesting. It might give me something to do on the plane on the way home tonight back to Mississauga.

This has been a fascinating study. I think all members of the committee, regardless of whether they're government members or opposition members, have really gotten a lot out of this. I think our goal on this whole thing is to make sure we don't stifle the creativity and the innovation, and what Canadians want out of social media, because they clearly want it. They're using it, they believe in it. It's an important communication vehicle for them through their friends, through their colleagues, and so on. But I think we want to make sure that we're also having a strong balance to make sure people's privacy is protected.

My oldest daughter is 13. She tweets, and I'm always worried, concerned as a father to make sure that her personal, private information is not part of it. Most of her tweets are fun little things. I think it's innocent and it's all good, but as a father I worry.

Have you been able to come up with policies within the organization to make sure that younger users of the service...? It's great for adults to send something out, or violate their own privacy. We're adults. We should take some responsibility. But when you have a 13-year-old daughter, you are concerned. You want to make sure she has some latitude and freedom to enjoy communicating with her friends through an excellent social medium, but you also want to make sure that their privacy is being protected. Do you differentiate in users around younger users of the system and people my age and others who really should know better in what they're sending and how their privacy is being protected?

**Ms. Laura Pirri:** Our service is not intended for users under 13, and we specify this in our privacy policy. If we do become aware that people under 13 are using our service, if that's brought to our attention, we will delete their accounts. We also provide resources for parents and teens. Those are linked to our privacy policy.

It's important for us to empower people to protect themselves on the service, and it's important for us to provide tools and features in

Twitter itself that actually do that. Our resources talk a little bit about this. Some of those features are, as I mentioned, you can protect your Twitter account such that your tweets are not publicly visible. If you're concerned about who might view them, you protect your account and approve who gets to see them. You can also block other users of the service if you don't like what they say. I also just think that the nature of following other users...because it's unlike other services, you don't have to follow me just because I follow you, so people can follow and "unfollow" at will. So if you don't like what someone is saying, it's very simple—

**Mr. Brad Butt:** Just on that, if someone decides to follow me, and I know you get the prompt—so-and-so is now following you—and it comes through, I don't have the right to say to them they cannot follow me. Is that correct? With Facebook, I can decide to make someone my friend or not, but if someone wants to follow me on Twitter, I can't block them from following me. Is that not correct?

**Ms. Laura Pirri:** You can block users.

**Mr. Brad Butt:** You can block someone from following you.

**Ms. Laura Pirri:** You can block users.

**Mr. Brad Butt:** I didn't think you could do that. I have some work to do when I get out of here. I'm kidding.

My last question is—

• (1600)

**Ms. Laura Pirri:** Sorry, you're saying if your account is protected, or are you talking about—

**Mr. Brad Butt:** Just a regular public account.

**Ms. Laura Pirri:** I'm sorry. You should protect your account if you don't want...otherwise it's public. Your tweets are public.

**Mr. Brad Butt:** If you reset your system to be a private account, you can block out anyone who decides to follow you. You actually have the ability to say, no, I don't want this person following me?

**Ms. Laura Pirri:** You have to approve them.

**Mr. Brad Butt:** All right.

When I get sent an email through my system and it's prompting me and suggesting that I follow so-and-so, how is that match being done? I assume that Twitter is looking at my profile as an individual, which some people could argue is private. I happen to be an MP and I'm married and I have kids, blah, blah, blah—and those are things I've done—but when I'm getting prompted that I should be following certain people because that fits a profile, is there a way to look at whether that violates any privacy rules? Obviously someone has made that determination in the back office that I should be following so-and-so because I happen to be a member of Parliament, or I happen to be a father or a hockey player, or whatever I am.

Where do you draw the line, as an organization, around those kinds of things, to make sure you're not stepping over? You're using private information about me and who I am to basically encourage me to be a more active user of the system. That's the whole idea of Twitter, right? It's to have more and more people communicating with more and more people. That's the whole idea.

Is there a way you strike that balance?

**Ms. Laura Pirri:** As I mentioned earlier, we don't require a lot of private personal information in order to use the service. A lot of our recommendations are based on who you are already publicly following, for example. Perhaps the people you're already publicly following are also publicly following...for example, if you happen to follow a lot of the same people someone else follows, we may suggest you follow some of the people they're following but you aren't already following, because we assume you are interested in the same—

**Mr. Brad Butt:** It's based on the public information I'm actually tweeting out, or things I'm following or receiving.

It's not based on my private profile as an individual—my private information. It's based on what I'm actually doing on your service.

**Ms. Laura Pirri:** You are not required to provide much private information, so we can make suggestions for you without having any kind of information about who you actually are.

That's how we're able to have anonymous users on our service. You can actually see in the suggestions that often they'll say “We suggest that you follow this person”. Then, we'll say that this person is already followed by other accounts and we'll show the photos of the people who are already following that person.

[Translation]

**The Chair:** Thank you.

I will now give the floor to Mr. Andrews for seven minutes.

[English]

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

Welcome, Laura.

I have a question on this anonymous part of Twitter. Have you reviewed how anonymous Twitter can be, and would you consider changing the business model to be not so anonymous, so for those who are posting on Twitter or commenting on Twitter, people can really know their true identity? Having said that, I also know that with Twitter you have verified accounts, official accounts, where I would assume it's been verified that they are those people.

How do you balance the two?

**Ms. Laura Pirri:** Clearly the verified accounts are not anonymous accounts, and for those accounts we think it is useful for other users of the service to know this is in fact that user. Having identity information for them helps provide users with an engaging service because they can find the celebrity or the politician they are looking for.

With respect to anonymous accounts, we believe there's a real value to allowing users to speak anonymously on our platform. It's something we're quite proud of. As a company, we've seen human rights activists or journalists in repressive regimes, for example, who are expressing unpopular viewpoints. It's part of our goal to be the platform to represent the stories and the voices of so many different users. We think it's important to allow those voices to be heard and for them to speak without providing identifying information that may have consequences where they may live. We've seen this in many cases over the course of our company's history, and it's something we're proud to provide.

•(1605)

**Mr. Scott Andrews:** Who decides whether a service is verified? Can a user decide they want their page to be verified, or is that something Twitter does if you get to a certain level of followers?

**Ms. Laura Pirri:** We have a help page that has information about it. Usually you do it at a point when you have a certain number of followers.

**Mr. Scott Andrews:** Can the user initiate that verified...?

**Ms. Laura Pirri:** The user can initiate it, exactly.

**Mr. Scott Andrews:** With regard to the direct message features of Twitter, one would assume that's private between two individuals, but there have been a number of breaches of the direct message services where I've gotten the same message.... It's like someone's been hacked, and blah, blah.

How often does this happen, and is it a major security concern of Twitter, how often these direct messages get hacked?

**Ms. Laura Pirri:** I'm sorry, what is the circumstance in which the message is...?

**Mr. Scott Andrews:** In direct messages, between two users on Twitter. In the last month or so I've received several messages from —

**Ms. Laura Pirri:** From people you're following already?

**Mr. Scott Andrews:** Yes, from people I'm following. I did not send them that direct message. How often does that service get breached?

**Ms. Laura Pirri:** I see, so it's a situation where the person you were following had their account compromised, and someone else sent the message.

Certainly, security is extremely important to the company, and we encourage our users to keep their own passwords secure and to enter in very secure passwords.

We are ourselves constantly providing additional security features for users. Unfortunately it does happen that sometimes people don't choose this—

**Mr. Scott Andrews:** How often does it happen?

**Ms. Laura Pirri:** I don't know. I don't have statistics offhand. But yes, if people don't choose secure passwords.... Whenever someone resets a password it goes through the process for when they believe their account's been compromised, and we do advise them on all of the best security practices to make sure that doesn't happen again.

**Mr. Scott Andrews:** It seems as if it happens more often, that it's quite frequent that you get these types of direct messages that were compromised.

**Ms. Laura Pirri:** Yes. Twitter is always working to try to protect against any kind of spam attacks as well, and trying to make sure user accounts aren't phished. This is something we constantly work on. We have a whole team in San Francisco dedicated to protecting security. We do try to make sure incidents like that don't happen.

**Mr. Scott Andrews:** You mentioned that you spoke with our Privacy Commissioner. Is the FTC your primary regulator for where you set the bar on privacy issues within the Twitter organization? Have you been dealing with any other privacy commissioners? Has Twitter been directed to do anything by any other governments in the privacy department?

**Ms. Laura Pirri:** We are a United States-based company, so the FTC is our privacy regulator. We are aware that we have users outside the United States even though our operations are in the United States and our headquarters are there. We are always open to collaborating with other commissioners and interested in privacy standards that are outside the United States.

As I said, trust is extremely important to us, so we are looking to do things, for example, implementing “do not track”, because we think that will build trust with our users.

We are open to being collaborative. We have not had any, I think you asked, dealings with other—

• (1610)

**Mr. Scott Andrews:** Other privacy commissioners or other FTCs?

**Ms. Laura Pirri:** No. We've had communications; we've reached out to people in the same way that we gave the Privacy Commissioner here a call, just to let them know we were launching this feature and supporting “do not track”. We've worked very collaboratively.

[Translation]

**The Chair:** I will now give the floor to Mr. Dreeshen for seven minutes.

[English]

**Mr. Earl Dreeshen (Red Deer, CPC):** Thank you very much, and it's great that you could be here today.

When we were in Washington, we had an opportunity to speak with the FTC, as Scott just mentioned, but also with some people who talked about the concept of privacy and perhaps looked at it in ways that not everyone has uppermost in their minds. They were talking about privacy versus fairness, inaccurate information being presented about oneself; seclusion, the right to be left alone; security, making sure that private information about your home and your family and so on is kept out of the media; liberty, the opportunity to be able to decide for yourself what you are going to be doing; and basic dignity.

These are the kinds of lenses that some of the people we were talking to asked us to consider, or at least keep in mind as we go through this particular study, because it is not one that is going on in different parts of the world.

How do you reconcile the use of your platform with some of the abuses of privacy, with some of those things that I've just outlined? Do you look at it a little differently for each of those aspects of privacy? Could you comment on that, please?

**Ms. Laura Pirri:** The abuses that you were mentioning....

**Mr. Earl Dreeshen:** There are the different aspects of it, different ways of looking at privacy, but we just use the one word to describe it. There are so many different levels, and I'm just wondering if there's an awareness of that or if you ever take a look at it through

that lens when you are trying to think about your privacy policies. That's why we are here, to take a look at the privacy policies and to see whether or not companies are flexible and are capable of reacting to new issues that might come up because they hadn't thought about them.

That's where I'm going with my question.

**Ms. Laura Pirri:** Yes, absolutely, I would say that a lot of the privacy principles that are being advocated in the United States as well are around not just notice, disclosure, security, information access, and the right to delete information or modify information. We certainly think about those things as well. Our privacy policy attempts to disclose to users all the different controls and tools that we give them around the information we collect, how it can be modified, and how it can be deleted. We give users those kinds of controls and that kind of access to the information we're providing on our service.

**Mr. Earl Dreeshen:** The other aspect of it is that people feel it is free; they're not paying every time, it's not like putting coins into a telephone. They have this concept that it is free, but of course you have to make money to function and to do as well as you do.

I noticed in some of the descriptions about the company, it says that Twitter does use cookie technology to collect additional website usage data and to improve its services. Could you outline for people so they really understand what your business model is? There's nothing wrong with that, and if it weren't for the fact that you could make money, it wouldn't happen. Could you give me a bit of background as to what you use and why you use it? Then perhaps people can get a better idea of what this free function is all about.

**Ms. Laura Pirri:** Sure; unlike other services, we don't have display advertising. We have what we call our own promoted products, which are organic and integrated into the Twitter service. The different promoted products we have are promoted accounts, promoted tweets, and promoted trends. Those are all parts of the Twitter service, and we just have a component of them that's promoted. We show people our promoted products in the same way that we try to show them other content that we think they may be interested in.

For example, when you see suggestions for accounts for you to follow, we may show you a promoted account in connection with other accounts that are not promoted. In the same way that we were talking about earlier, we may suggest that you follow particular accounts because people you are already following have already followed those accounts; we might do the same thing with a promoted account.

For example, I follow a bunch of lawyers, a bunch of technology journalists, and some privacy researchers. These people may be following an account that is an upcoming privacy conference. Perhaps the privacy conference has decided to promote its account, given that the conference is coming up and they want more people to be aware of what's going on, so that might show up as a promoted account.



•(1615)

**Mr. Earl Dreeshen:** If somebody was re-tweeting an article they'd read, would you have a way of tracking that? I mean, this is the use, through your platform, of someone else's...and of course there's advertising taking place, perhaps, if you are sent to another media source or whatever.

Is there a way that this would be tracked through your service, or is it just a case that you get a chance to use it and that's good enough? Do you have a way of continuing out, just to see how it's being used in different media?

**Ms. Laura Pirri:** Do you mean outside the Twitter service?

**Mr. Earl Dreeshen:** Yes. I'm just wondering; you had the platform there, which allowed it to be directed there—

**Ms. Laura Pirri:** To my privacy conference, let's say—hypothetically.

**Mr. Earl Dreeshen:** That's right.

**Ms. Laura Pirri:** No, not off the Twitter service. I gave the example in my opening comments about Twitter when integrated into other services; we'll receive web visit information in those kinds of situations. Otherwise we will not know off Twitter.

[Translation]

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

I will now give the floor to Mr. Boulerice for five minutes.

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

Good afternoon, Ms. Pirri. Thank you for being here. It's much appreciated.

Like many of my politician colleagues, I use Twitter a lot, of course. You have revolutionized political communication by forcing us to express our ideas in 140 characters. We now have to express our ideas concisely.

I will come back to an issue which was raised by my colleague.

You provide consumers and citizens with a free service. As well, there really isn't any advertising on Twitter, as opposed to Facebook, which does a lot of advertising. I still don't really understand where you make your money.

[English]

**Ms. Laura Pirri:** Well, we do make our money from our promoted tweets, our promoted trends, and our promoted accounts.

[Translation]

**Mr. Alexandre Boulerice:** What I'm interested in, because it is part of our study and because we will be hearing from witnesses on this subject this afternoon, is whether you collect information on people who have a Twitter account, and whether you sell this information to data brokers.

[English]

**Ms. Laura Pirri:** No, we do not.

[Translation]

**Mr. Alexandre Boulerice:** You don't do that?

[English]

**Ms. Laura Pirri:** We do not do that.

[Translation]

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

A little earlier today, I engaged in a fun little exercise. I used my Twitter account to ask people to suggest questions I could ask you, and I got some replies. People responded.

[English]

**Ms. Laura Pirri:** Great.

[Translation]

**Mr. Alexandre Boulerice:** Maryse Tessier, who is a reporter with *La Presse*, a daily newspaper, asked me to ask you the following question: what are you doing to prevent people from posing as someone else? For example, if there was a Twitter account in the name of Alexandre Boulerice...

**An hon. member:** Or of Justin Trudeau...

**Mr. Alexandre Boulerice:** No, not Justin, just me. In short, how can people know that it's really me? Otherwise, my reputation and my image could be affected if someone else writes terrible things by posing as me.

[English]

**Ms. Laura Pirri:** That would be in violation of our Twitter rules. We do not allow people to misrepresent the identity of other people in a way that is, as you suggest, misleading. If that account were reported to us, we would take that account down.

[Translation]

**Mr. Alexandre Boulerice:** All right, I would have to complain. Someone from your department would investigate. Is that right?

•(1620)

[English]

**Ms. Laura Pirri:** Exactly.

[Translation]

**Mr. Alexandre Boulerice:** So there is a mechanism.

[English]

**Ms. Laura Pirri:** That's correct.

[Translation]

**Mr. Alexandre Boulerice:** In the course of our discussions, we talked about the problem of intimidation, especially among teenagers. I would like to know whether you have any measures to counter that. For example, a gang at school could use Twitter to attack someone, to make them look bad. Do you have any mechanisms to try to block that, if it is reported?

[English]

**Ms. Laura Pirri:** Our philosophy around that is to empower people to have the tools to do it themselves, to protect themselves. That's where the protected accounts come in, and the ability to block particular people. You can be anonymous on the service. You can not agree to let other people see your tweets if you're a protected account.

We have resources for teens. If there is harassment targeted at particular individuals, then that's a violation of our rules. We don't allow that if that is brought to our attention.

We also provide resources on our service for parents and teens to help them deal with these kinds of situations. Blocking and ignoring: that's often what we find to be the most effective way to go. Often if you actually ask for content to be taken down, it just makes the person who is the bully feel as though they were successful in what they were trying to accomplish. They may create another account and then try to do it somewhere else.

So blocking and ignoring—that's usually what we recommend people do.

[Translation]

**Mr. Alexandre Boulerice:** I only have a few seconds left. So I will share a final observation with you, which is that you have turned me into a completely impatient person. I cannot wait anymore to see what a reporter will write in an online piece: I immediately turn to Twitter to see what is being reported. Thank you for making that possible for me.

**The Chair:** That's absolutely normal. I do the same thing.

I will now give the floor to Mr. Mayes for five minutes.

[English]

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

Thank you to our witness for being here today.

The issues we have been reviewing are about how we are going to monitor privacy violations. Then, of course, in the delivery in social media is the simplicity of consent as far as the collection of data or marketing of data is concerned—those types of issues.

I'm just wondering about this. In listening to what you've explained to the committee here, I almost see that there's a responsibility of the user to protect their own information, because they're the ones who are supplying that information to the platform. It would almost be impossible to monitor 400 million tweets in...is it in a day?

**Ms. Laura Pirri:** Yes.

**Mr. Colin Mayes:** Yes, so I guess that's the issue I have. As far as any of your customers who would complain about violations of privacy go, your natural defence would be that it's your responsibility as an individual user to not disclose things that you don't want to be viewed by the general public. Would that be your defence?

**Ms. Laura Pirri:** Well, I think this gets back to our privacy philosophy. We think it's really important that it be clear with users why we're collecting the information and how it gets used, and that

we give them abilities to delete the information and to do so in a way that's more granular than just deleting your account. We try to do things that are a little more fine-tuned, such as how you can delete the location from your tweet without actually deleting the tweet itself.

That's where we think that if you give users options like that, it helps them make informed decisions, and they're then empowered to protect themselves.

**Mr. Colin Mayes:** Any problems would be complaint-based, though, wouldn't they? Because you couldn't monitor something like Twitter for privacy. It would be impossible.

**Ms. Laura Pirri:** Yes. For example, for violations of our rules, we do have a process for people to submit complaints to us, and that's how we respond to them, given the volume of content that we have on our service.

**Mr. Colin Mayes:** Previous testimony by a lawyer was that the disclosure and the customer agreeing to certain conditions of the use can't be concise because there are so many legal things that have to be covered. Quite often, people just go through it and say "I agree"; they don't read it.

Has your company made any effort to try to be a little bit more simplistic in your consent that you provide to people? I really think the big issues are the collection of data, the marketing of data, and also the term of the retention of the data. Those are the three big ones, I think, for customers. Have you been able to do anything with regard to that?

• (1625)

**Ms. Laura Pirri:** Yes, and perhaps it's not surprising that since we're a service that's about simplicity and 140 characters, we do favour brevity. We've taken great pains to try to make our privacy policy shorter than many, and we are very user-friendly in the language we use.

We also think it's important for users to have access to more information about certain features, so we'll link from our policy to the help pages, which have additional specifics. Then, as I mentioned, we also provide additional disclosures in the context, in the product, so that the user doesn't have to dive into some long privacy policy and find the exact section where the company is treating your information is mentioned.

**Mr. Colin Mayes:** Do you have any recommendations for the committee—your thoughts, through your experience—on ways in which we can ensure that customers' privacy is protected not only in the delivery of your service but also in other services?

**Ms. Laura Pirri:** I would certainly say that our experience—for example, with the product launch I mentioned—really was doing privacy by design. We did it in a very collaborative way with the U.S. FTC and with others in the privacy community.

Being able to have that kind of back-and-forth relationship as we went through the product development cycle was extremely useful. We felt we could be really open and candid. We got a lot of feedback through that product development cycle that we incorporated, such that the final product we launched was different from the one we were thinking about when we went into it at the beginning.

Having that kind of input and engagement is really useful in making sure that you don't miss things, and that when you're trying to do the right thing you're able to execute it, and you don't have any surprises down the road.

[Translation]

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

The last few minutes of our first hour will go to Mr. Larose.

**Mr. Jean-François Larose (Repentigny, NDP):** Thank you, Mr. Chairman.

[English]

Thank you to our guests for being here. I appreciate it.

[Translation]

I am also on Twitter. As well, I am a member of Parliament who believes in the democratic process around the world, in the free flow of information and in freedom of expression. This is very important. It helps us improve our world and our planet, but at the same time, it raises some questions for me.

I've been listening to you from the beginning, and I have some concerns. I'm thinking of the role Twitter played when some regimes were challenged. It was a passive participation, but the free flow of information weakened some regimes. You are not the only ones, because there are other networks.

You have been very successful and you have been a victim of your own success. Given how much you have expanded, have you brought about mechanisms to protect yourself from people who are very disturbed by your very existence and who might engage in computer attacks? Of course, I am referring to what happened in January and May 2009 with regard to certain individuals. In that case, individuals were involved, but my question has to do with much bigger actors, who have a lot more money.

[English]

Do you want me to say it in English?

**Ms. Laura Pirri:** No, I'm just trying to make sure that I understand.

Is your concern about certain communications or is there...?

**Mr. Jean-François Larose:** Have you put mechanisms in place to protect yourselves?

**Ms. Laura Pirri:** Do you mean protect Twitter, as a company?

**Mr. Jean-François Larose:** Yes.

**Ms. Laura Pirri:** What do we need to protect it from?

**Mr. Jean-François Larose:** I mean protect it from cyber attacks.

**Ms. Laura Pirri:** Oh, so you mean security-related?

**Mr. Jean-François Larose:** Yes. I don't mean individuals, but bigger actors around the world, because you are becoming global.

**Ms. Laura Pirri:** I see. Absolutely.

As we grow and become bigger, security and having secure systems are enormous priorities for the company. Security has actually been a priority for the company in the last couple of years, as we've been scaling up just to handle the enormous volume of

tweets we've had. We have just had to scale our infrastructure, and part of scaling the infrastructure is also making sure that it's very secure. As I mentioned, we have a dedicated team in San Francisco constantly looking at these issues and trying to make sure that the service is protected against spam or against any particular security threats.

Certainly that is something for us to be thinking about.

•(1630)

[Translation]

**The Chair:** I would like to ask a brief question before we conclude.

[English]

**Ms. Laura Pirri:** Of course.

[Translation]

**The Chair:** I would like to use my prerogative as chair to ask you a question, but also in my capacity as a Twitter addict.

I'd like to talk about the pictures that are on Twitter. Once they are up, do they belong to you? If users publish pictures, do they still have rights to those pictures?

[English]

**Ms. Laura Pirri:** I see.

You retain the rights to the content that you submit to the service, as is written in our terms of service. You do give us permission, so you give us a licence, to distribute it on the service.

This is an issue that Twitter is actually litigating in a court in New York at the moment. A court found that a user did not have standing to contest the provision of their personal information, because the user didn't have any right to or interest in the contents of their Twitter account. So Twitter said, "No, as a matter of fact, under our terms of service, users do retain the right to the content—so their content, including their photos—that they submit to the service".

[Translation]

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

Our time is up, and we will now suspend our meeting for a few minutes. We will then start the second hour, during which we will hear from our second witness via videoconference.

Thank you once again for having appeared before the committee, it was greatly appreciated.

•(1630)

\_\_\_\_\_ (Pause) \_\_\_\_\_

•(1635)

**The Chair:** We will now begin the second part of the meeting.

I have the pleasure of introducing Ms. Barrett Glasgow. She is a spokesperson for Acxiom and is speaking directly from Washington, DC.

We will proceed the same way we did earlier. The witness will have 10 minutes to make her presentation, and then there will be a question and answer period with the committee members.

So without further ado, I would like to welcome Ms. Barrett Glasgow and I would like to thank her for being here. Ms. Barrett Glasgow, you have 10 minutes.

[English]

**Ms. Jennifer Barrett Glasgow (Global Privacy and Public Policy Executive, Acxiom):** Thank you.

Chairman Dusseault, Vice-Chairman Andrews, Vice-Chairwoman Davidson, and members of the committee, thank you for the opportunity to share Acxiom's perspective. Also, thank you for the opportunity to do it via video conference.

First, let me say that, as a global company, protecting privacy has been a priority for Acxiom for decades especially in countries unlike Canada where the laws do not cover all of the uses of personal data. We as a company pride ourselves on following all the legal obligations in each country where we source data. I also want to point out that when consumer data is properly used it can make significant contributions to the economy, and the growth and stability of an economy.

For 40 years Acxiom has been a market leader in responsibly providing innovative, computerized marketing services and a complementary line of data products to help our clients deliver better products and services smarter, faster, more cost effectively, and with less risk. Our global revenues are in excess of \$1 billion annually. Our computerized marketing services are over 80% of worldwide revenues and our data products are less than 20%.

While in other countries we do provide a wider range of products and services, in Canada we only provide business and consumer telephone directory products amounting to just under \$1.5 million in annual revenue. Acxiom does not have a physical presence in Canada. Instead, we deliver and support our Canadian business from our headquarters in Little Rock, Arkansas, here in the U.S.

Acxiom's Canadian business and consumer directories are licensed to companies and non-profit organizations for their internal use as an automated and inexpensive form of directory assistance or for direct mail and telemarketing purposes. Our directories are also licensed to companies that host directory search engines on the Internet for both consumer and commercial use. In these instances Acxiom's listings may be merged with telephone listings from other sources by our client. Many of the sites that license our directories display on the side the reference, "Data by Acxiom". Our clients receive updated replacement directories on a periodic basis, some monthly, some quarterly, and others less frequently. These directories contain published business and consumer listings from printed telephone directories and additional listings available from directory assistance. They also contain Canadian census data that has been appended to the listings. We also flag all consumer records that have registered with the Canadian Direct Marketing Association through their do-not-call and do-not-mail suppression services. All clients who use the directory for telemarketing purposes must also use the Canadian national "do not call" list to block calls if the company does not have an existing business relationship with the consumer.

For our Canadian consumer directory, we offer consumers the ability to have their listing removed or, in other words, opt out, at no charge. For our Canadian business directory we offer the ability to

remove or correct an inaccurate listing at no charge. In addition, if the business so requests, for a fee, we will publish a corrected yellow or white page listing to all our clients who get our business directory. Business owners and consumers can contact us by calling our consumer care department at a 1-877 number here in the U.S., which works in Canada. They can also opt out of our directory products by going online to Acxiom's corporate website, www.acxiom.com, and completing an opt-out request form. We also ask any client who uses our data to refer a consumer to us who asks about the source of the data. Opting out removes the listing from the next monthly maintenance cycle for the directory and our clients receive the update in their next scheduled update cycle. We also inform consumers who want to have their data removed from the Internet that they should contact the directory search engines directly. If they want their data removed more quickly then the site will receive an update from Acxiom.

• (1640)

This is a wise step to take, because there are other providers of such directories, and the search engine may not have gotten the listing exclusively from Acxiom.

As I hope our comments illustrate, Acxiom has a culture of respecting consumer privacy, and where laws exist, of honouring the obligations the law places on us and our clients in using personal data. Informational hearings such as this one are very helpful in informing all parties about how personal information can be appropriately used.

Mr. Chairman, I appreciate the opportunity to appear here today and am available to provide any additional information the committee may request.

Thank you.

[Translation]

**The Chair:** Thank you for being here.

And now, we will hear from Mr. Angus for a seven-minute turn of questions and answers.

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

[English]

Thank you, Madam Barrett Glasgow, for joining us today. We are very pleased to have you at our study.

As you know, this parliamentary committee is looking at the issue of new media, primarily social media, and the data information being put out there. How is it being collected, and how are we protecting privacy rights without being overly intrusive? If data is compromised, all manner of criminal acts can happen against individuals.

We're very pleased that you are being represented today. Your company has been called "Big Brother in Arkansas". You are the biggest data broker in the business. Is that correct?

**Ms. Jennifer Barrett Glasgow:** I don't know that we're the biggest, but we are one of them, certainly in the U.S.

**Mr. Charlie Angus:** There are 500 million people and 1,500 data points of information per person. That's what we're being told. You have sales of \$1.13 billion.

I just want to clarify. Are you gathering the kind of general information on Canadian citizens you would gather on American citizens? When I look at 500 million people, that's the size of continental North America. How much Canadian data is in there?

**Ms. Jennifer Barrett Glasgow:** We only have Canadian data from the telephone directories I described in my opening remarks. The 500 million names represent our worldwide consumption. Acxiom has offices in Europe, the U.S., Latin America, and Asia.

**Mr. Charlie Angus:** It's telephone data. Okay, thank you.

I'm looking at some of the briefs I have read on various big data companies. I'm certainly not saying that Acxiom is a bad player, but there have been some examples of problems. We're trying to get our heads around what big data does.

If we have 1,500 points of data on individuals, that would seem to be a lot of information. The data brokers collect general land title information, birth records, licences, court records, telephone directories, and non-public information that can come from loyalty card purchasing histories, consumer surveys, warranty restrictions, and information from magazine subscriptions. Then, through cookies, they are able to track browser use on the Internet. Would Acxiom be doing that with U.S. consumers?

**Ms. Jennifer Barrett Glasgow:** In the U.S., not in Canada, we collect data from all of those sources, except for browsing data. We do not collect cookie data that tracks the browser history of individuals.

**Mr. Charlie Angus:** I'm pleased to hear that, because I find it personally to be very disturbing. I sometimes try to go on a website, and because I like to have my cookies turned off, I am told that I can't access it unless the cookies are on. That somebody would be gathering information on my browsing data I would find very disturbing. I am pleased to see that Acxiom doesn't do that.

Are you looking to expand the data sets you have on Canadians, or are you going to stick with the telephone directory?

• (1645)

**Ms. Jennifer Barrett Glasgow:** The telephone directories have been our offering in Canada for over a decade. We don't have any plans to expand that. The market is not a large market for us, so our focus has been elsewhere.

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

Within our privacy regime—and we're looking at possible changes to our privacy regime to protect data—the question of breaches is enormous. There have been some pretty dramatic examples. We found out that in 2005, ChoicePoint sold the information of 160,000 people to an identity-theft ring. In 2004,

the same company was involved in a breach of the data of over 128,000 citizens.

What does Acxiom do to protect personal data? I'm sure that you have pretty strong firewalls. Have you had breaches? What happens in the case of these breaches?

**Ms. Jennifer Barrett Glasgow:** We have a very strong commitment to security, not so much for our data business, but for our services business. We host and provide marketing services to a lot of regulated industries, such as financial services and health care. As a result of that, those industries audit our security practices regularly. We have over 80 outside customer audits a year. Then, of course, we do our own audits. We're always testing our security, always upgrading our security, because we take data breaches very seriously.

I would say that we have the normal kinds of situations that most companies do, with lost laptops, but we have a very strong encryption policy where all data that is in removable form is on an encrypted device. We minimize the risk when an employee has a device that's lost or stolen.

**Mr. Charlie Angus:** Again, with the data points, your catalogue is pretty impressive in terms of what you can offer clients who are gathering information on all manner of ethnicity, gender, neighbourhood.

The rules may be different in Canada, but in terms of the ability to actually target by race and ethnicity, have you had any questions from the FTC about the appropriateness of that?

**Ms. Jennifer Barrett Glasgow:** Well, there are certain industries that by law are barred from targeting by race or ethnicity. Financial services happens to be one of those. But for other industries, particularly consumer product industries—for example, cosmetics, which are developed specifically for some ethnicities—there's actually a consumer benefit to target. It does vary from industry to industry.

**Mr. Charlie Angus:** For your clients, people who are wanting to sell products, it makes sense that they're going to want to know who is in certain markets. Can individuals buy data?

**Ms. Jennifer Barrett Glasgow:** No, we do not sell to individuals, we sell only to qualified businesses. We carefully screen all of our clients before we sell any products to them to make sure that they are a legitimate business and that they have a legitimate name for the data they're specifically requesting.

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

[*Translation*]

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

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

**The Chair:** Ms. Davidson now has the floor for five minutes.

[English]

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

And thanks very much, Ms. Barrett Glasgow, for joining us this afternoon. We certainly appreciate hearing from you. I think we're getting a different perspective on another part of this study on social media.

You've said that you're a global company; that you certainly follow the rules in all of the countries that you operate in; that you aren't in Canada physically, that you monitor the Canadian operation through Arkansas; and then you talked about your business in Canada using the phone listings and the 411 listings and so on.

Can you talk about that a little bit more? Just describe to me a bit more what your business is in Canada, and how your business in Canada interacts with social media.

• (1650)

**Ms. Jennifer Barrett Glasgow:** The business in Canada is just a telephone directory service. As I said in my opening remarks, it includes public listings, so anyone who's not listed or available through directory assistance would not be found in those directories. Consumers can choose to get out of them. We have the same directory service in the U.S., and we find consumers who don't mind being in a printed telephone directory, but are uncomfortable being in an Internet directory.

Many of the clients we have are actual Internet search engines. When you go to places such as yellowpages.com and so on, you would potentially be searching data that was provided to those search engines by Acxiom. We keep that data updated and refreshed as the directories are updated and republished.

The difference between the Canadian data and the U.S. data is quite substantial. The previous member was just outlining some of the things we do in the U.S., and we do some of those other activities in Europe and in Asia as well, maybe not quite to the extent that we do in the U.S., because that's where the company started.

In terms of interaction with social media for our Canadian business, there really isn't any, unless, from a user standpoint, social media would like to take information they find in a social media account and cross-reference it against a published directory. We don't link data between social media and these directories.

**Mrs. Patricia Davidson:** Have you been following the study we're doing or are you aware of the study we're doing?

**Ms. Jennifer Barrett Glasgow:** I'm only generally aware of it. I have not been following the details.

**Mrs. Patricia Davidson:** Okay. I'm just trying to see how your business relates to our study when we're looking at protection of privacy and social media and so on. I'm hearing from you that you don't necessarily have a connection with social media.

**Ms. Jennifer Barrett Glasgow:** I don't really think we do in Canada, and I think that's because of the limited products we offer in Canada. In the U.S. we have products that identify heavy users of social media and what types of social media, such as Twitter or

Facebook, an individual might use, but we do not offer those kinds of products in Canada.

**Mrs. Patricia Davidson:** In your opening remarks you talked a bit about removing and opting out or removing and correcting, I believe, if it was a commercial operation?

**Ms. Jennifer Barrett Glasgow:** Yes.

**Mrs. Patricia Davidson:** Could you just elaborate a bit more on that?

**Ms. Jennifer Barrett Glasgow:** Consumers who want to have their telephone directory listing removed may have it removed from the directories we sell for the search engines or they may have it removed from all of the directory products, things that are used for direct-marketing purposes rather than just directory search engines. They can contact us to do that via our website. They can fill out the form online and that opt-out is posted in the next update cycle of our database, which is monthly, and then redistributed to our clients.

For the business side of the house, we offer essentially the same service, but because businesses really don't typically want to opt out, they usually contact us if they've moved or changed their telephone number or something. They're typically more interested in a correction, because businesses want consumers to find them. We will make that correction, and it will be published in the normal update cycle, but if they want us to do a special distribution of that new data, then we do ask for a small fee for that.

**Mrs. Patricia Davidson:** This is your Canadian business that you're referring to right now?

**Ms. Jennifer Barrett Glasgow:** It's for the Canadian directories. That's correct.

**Mrs. Patricia Davidson:** I don't think I have any other questions at this time.

Thank you very much.

[Translation]

**The Chair:** Thank you, Ms. Davidson.

Mr. Andrews now has the floor.

[English]

**Mr. Scott Andrews:** Thank you, Jennifer, for being here with us today.

You said your information for Canada is limited to the directory and the census, but are there Canadians doing business in the United States through different companies or different loyalty programs or those kinds of things whose data you might actually catch through a company or an organization that they're doing business with in the United States?

• (1655)

**Ms. Jennifer Barrett Glasgow:** Well, if we did, if some of our sources provided us data on Canadian citizens, then we would screen them out when the data came to us to put into our products.

Each of our products in each country is built for that country, so that we can be sure we're complying with appropriate laws relative to citizens' data.

**Mr. Scott Andrews:** So you'd screen out Canadian data?

**Ms. Jennifer Barrett Glasgow:** Yes. If we bought a list from someone that had both Canadian and U.S. data in it, we would exclude all of the Canadian data when we built our U.S. product.

**Mr. Scott Andrews:** Okay.

We heard a lot about data matching and getting information from five, six, or seven different sources and then data matching people based on partial information or bits and pieces. Could you explain to us a little how exactly that process works?

**Ms. Jennifer Barrett Glasgow:** Yes. Let me start with Canada, because it's pretty simple, and then I'm happy to describe what we do in the U.S., which is far more complex.

In Canada, we match name and address and telephone number, because these are telephone directory listings and we have a phone number for every record.

We append census data to that based on geography.

We would take your census file, which is at a geographic level, and then we would append census characteristics to the individual record. If someone were using it for direct marketing purposes or telemarketing purposes, they would have more information about the individual than just their name, address, and phone number. That's a fairly simple process.

In the U.S. and in other countries, we will match names and addresses. We will match telephone numbers when we have them. When we're not dealing with directories exclusively, we may have records that do not have a telephone number on them.

We would use the highest, most accurate information we have available in the record. Part of our matching algorithm—I think it's something that any good data company that collects and assimilates data from multiple sources needs to do—is to have quality standards related to the data integration or data matching.

For instance, take an initial; my name might come in from one source as "J." Glasgow, or it might come in as "Jennifer" Glasgow. If I lived in an apartment building, I might have the street address but be missing the apartment in one record. We would go through a data hygiene process to try to standardize and clean up, to the degree we can, any inconsistencies in the address or misspellings of maybe street names or other things like that. Then we would match records together to try to determine if we have information about the same person or household from multiple sources that could be integrated together to build a composite of information.

That's how we get, as the earlier member discussed, up to 1,500 different data elements on one individual and household.

**Mr. Scott Andrews:** Thank you very much.

[*Translation*]

**The Chair:** Mr. Kramp, do you have a question?

[*English*]

**Mr. Daryl Kramp (Prince Edward—Hastings, CPC):** I would like to maybe dovetail the privacy issue with the security issue.

Where does your hardware and software come from? Where does it originate? What is its proprietary nature? Is it U.S.? Is it Asian? Is it European?

**Ms. Jennifer Barrett Glasgow:** It's primarily U.S. Our largest data centres are in the U.S., but we do have data centres in the U.K. that service our European operations. We have data centres in Australia and China that service our Asian operations.

The data centre for all of the processing we do for Canada is based out of one of two locations in the U.S.—either our Chicago data centre or our Conway, Arkansas, data centre, which is just outside of Little Rock, our headquarters, where I reside.

**Mr. Daryl Kramp:** Thank you.

**Ms. Jennifer Barrett Glasgow:** The software is commercially available software from IBM, from Oracle, from SAS, and others.

**Mr. Daryl Kramp:** The reason I'm wondering is that obviously we have heard a lot of discussion...certainly in the U.S., where an election has just passed. On a consistent basis, though, both political and business interests in the U.S.A. have expressed concerns regarding security, particularly with regard to the interaction with the Asia-Pacific region.

Would you like to comment on that?

**Ms. Jennifer Barrett Glasgow:** We certainly understand the concern, having a footprint in Asia, in both China and Australia. We have firewalled all of our different operations. We limit access by employees who have access to servers or to systems, or who do maintenance on servers and systems by region as well, because we're sensitive to all of those concerns.

In terms of many of the requirements we follow for our clients in regulated industries, such as financial services or health care, we don't segment the client processing out separately from other industries, so other industries, such as retail, telecommunications, or the catalogue industry, enjoy the benefit of those higher security standards from those regulated industries.

● (1700)

**Mr. Daryl Kramp:** I'm just wondering how confident you are in your firewalls, particularly when the interaction now of course encompasses the entire financial sector, the insurance sector, telecommunications, and all of the technology companies. If there is any concern at all with regard to firewalls, I would suggest that perhaps some of the people who have registered international security concerns....

Have you been able to alleviate all of their concerns, or is there any lingering doubt?

**Ms. Jennifer Barrett Glasgow:** We have alleviated all of the ones that we're aware of, but I will reiterate that it is a continuing, iterative process, which is why we do audits ourselves. We do all kinds of data loss prevention, as well as firewall and on-site security checks daily, so that as the threats evolve, which they do over time, we're always at least one step ahead, if not further ahead, of the bad guys.

**Mr. Daryl Kramp:** The reason I asked is that I have some responsibilities here as chair of the Canada-China relationship. As such, there is a lot of interaction, and there are concerns registered between technology companies, whether it was Data Comm with the Huawei corporation and/or others.

Knowing that in the Asian market right now there is such an abundance of new players on the scene in the transmission of data, whether it's through the Philippines or wherever, I would really, really like to be assured that with the scope and the market share you have, you feel very confident that, should Canada have any interaction at all, even to a greater extent than we do right now, obviously the assurance is there that your security is absolutely flawless.

**Ms. Jennifer Barrett Glasgow:** Well, "flawless" is a word that I'm not sure applies to security these days, unfortunately, but we take every precaution we can. As I said, we're constantly checking it and we have the added value of having our clients come and check us as well.

**Mr. Daryl Kramp:** Thank you very much.

[Translation]

**The Chair:** Mr. Boulerice now has the floor.

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

Thank you for being here. I have to admit that I did not know of your existence until the committee started its study on privacy and personal information.

You have data on 500 million people. You could have up to 1,500 different data points on each of these people. You learn a lot about someone if you have 1,500 data points about them. That's quite an achievement. How do you collect all this information on all of these people?

[English]

**Ms. Jennifer Barrett Glasgow:** Let me maybe clarify the 1,500 data points. That is the maximum number of data points that we attempt to collect. I don't know that we have all 1,500 elements on any one individual.

About half of those are actual interests and activities that consumers are involved in and, of course, while I may play golf, I typically may not also play tennis or boat or have other hobbies. The average number of elements on any one individual is certainly not nearly that high. I would say that it's maybe more in the category of several hundred.

Also, I think it's important to understand that it is a description of our U.S. products, and that is the business that has been around the longest—for over 40 years. We have more recently expanded into other geographies—Canada, Europe, Latin America, and Asia—and in those countries, we have far fewer information points.

• (1705)

[Translation]

**Mr. Alexandre Boulerice:** How do you know whether someone plays golf rather than tennis?

[English]

**Ms. Jennifer Barrett Glasgow:** The data in the U.S. comes from three primary sources. It comes from public records, but for something like golf or tennis, it would typically come from a consumer survey in which they have indicated that this is an interest of theirs. Or it would come from a subscription to a golf or tennis magazine, or purchases from a golf or tennis catalogue.

[Translation]

**Mr. Alexandre Boulerice:** When I was going over your client list, to whom you sell information on individual profiles, I noticed that HSBC was on the list, and this bank is suspected by an American senate committee of having indirect links, but potential links, with Mexican drug cartels.

If you really want to protect the privacy of these people, how can you ensure that your clients protect the personal information of hundreds of thousands of people, even millions of people? Indeed, once you've given the information to HSBC, how can you know what the bank will do with that information? If there is illegal activity involved, it's potentially dangerous.

[English]

**Ms. Jennifer Barrett Glasgow:** We provide data to any client—HSBC or any other client—under contract, and that contract specifically says what they can do with the data. In the case of our U.S. clients, they can use the data for marketing purposes. They typically do not receive all of those data points. They are interested in certain data points for their particular marketing purposes, and not all data points are applicable to all industries.

They would receive a subset of the data, and they would have a requirement from us to use it for a period of time and to either return it or destroy it. For our larger clients we actually often have on-site employees of Acxiom who work at the client's location who give us added assurances that those contractual terms are being followed.

[Translation]

**Mr. Alexandre Boulerice:** For the purposes of our study, I would like to know whether you have a business relationship with social media companies like Facebook or Google.

[English]

**Ms. Jennifer Barrett Glasgow:** We do provide some data to Google and Facebook. As I said earlier, we indicate through surveys and other non-social media services or sites that people have an interest in social media, a high or low interest, and what kinds of social media, such as Twitter or other chat rooms, as opposed to, say, a Facebook-type of social media. But we do not integrate data from those sites into our products.

[Translation]

**Mr. Alexandre Boulerice:** That's it? All right.



**The Chair:** Mr. Angus would like to clarify a point.

You will be the last one. There still is some time left.

[English]

**Mr. Charlie Angus:** Thank you, Madam Barrett Glasgow. We're really pleased that you participated in this. We have a lot of concerns about the role of big data, and you put a face to it. I can say—no offence to your company—that I'm kind of pleased that Canada is so small in your world that you just have my telephone book information. Thank you for that. If you ever decide that we're a little bigger in your world, please let me know. I'd certainly be inviting you back to our committee.

I'm looking, then, mostly at what you're gathering in Europe and in the United States for information. I'm looking at your catalogue and what you offer, your customer data products catalogue.

People can gather a phenomenal amount of information from this. I know not everybody has 1,500 data points; I don't know if I have 1,500 data points in my life, but maybe I do. But I see allergies, seniors' needs.... If you're getting people's records, their phone records, their allergies, their ethnicity, when someone buys that data, do they get the names with that, or do they just get aggregate data with the names stripped out?

**Ms. Jennifer Barrett Glasgow:** No, they typically get the names. The data is delivered to the clients in two ways. They can buy a list from us that is a selected list based on certain criteria that they specify. In other words, a drug company might want a list of people with an interest in allergies or who suffer from allergies, because they want to promote a particular new product to them. We would select those people from our database and send that client of Acxiom's the list, and it would include the names and addresses. It might include the telephone numbers if they're intending to do a telemarketing campaign.

The other way they can receive data from us is through something we call "list enhancement". That is where our client, in this case the drug company, would send us the names and addresses of people they are looking for allergy data on, and we would match those to our database and append the data that they specifically have requested—in this case, interest in allergies—to their list, and send that list back to them.

• (1710)

**Mr. Charlie Angus:** So if I have a loyalty card and I'm picking up medication, and that data is being put together and someone buys a list, they know what I'm taking?

**Ms. Jennifer Barrett Glasgow:** No, any of the health-related information comes from surveys. It does not come from protected health information. In the U.S. we have a law called the health information portability and accountability act, HIPAA, which regulates prescription information and patient-doctor information. This information would have come from a consumer filling out a survey saying they either suffer from allergies or have an interest in allergy products because of someone in the household who does.

**Mr. Charlie Angus:** But you're saying you don't separate the data points out so that if we start to identify that Joe Blow goes to the liquor store and uses his air miles points to buy his liquor every week, that's put in the data. We know that he's been divorced because

we have the divorce records. We know where he lives. You don't separate the name information from what they do. That can all be purchased.

**Ms. Jennifer Barrett Glasgow:** The type of data you just described, such as what he purchases at the liquor store and so forth, would not be the type of data that Acxiom has. We have general demographic information that describes the household characteristics: is this a couple living there? Do they have children? Is it an older couple or a younger couple? It's that type of thing, and then we would have interests and lifestyle information, not related to any kind of sensitive or health or financial types of transactions. It's general in nature, but it is associated with the actual names and addresses.

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

[Translation]

That's all the time we have, unless there is another question.

Thank you very much for your time and for having appeared before the committee today. We are going to carry on with our business.

[English]

**Ms. Jennifer Barrett Glasgow:** Thank you.

[Translation]

**The Chair:** However, I would ask committee members to stay for another couple of minutes to discuss another matter.

I would just like to ask you to think about what our next study could be. As you know, we are hearing the last of the testimony. So when we come back from the Christmas break, we'll have to begin a new study. So we will have to think about that. We will probably have some time to discuss that at the next meeting, which is next Tuesday. At that point, we will hear from the access to information commissioner, who has managed to find some time in her schedule to see us.

I just wanted to let you know about that.

Further, no one from Microsoft or Apple will be able to come. That is the other thing I wanted to tell you. In fact, that's about all I wanted to say.

So, for your homework, you will have to think of another subject we could study when we come back after the holidays.

Mr. Warkentin, go ahead.

[English]

**Mr. Chris Warkentin (Peace River, CPC):** I just wanted to mention that we would be discussing with the opposition what might work in terms of the year, and so we'll do that, but we also wanted to clarify that it is confirmed that we're not meeting on Thursday.

[Translation]

**The Chair:** Unless the committee states otherwise or something comes up, we will not meet on Thursday, December 13.

[English]

**Mr. Chris Warkentin:** I just wanted to confirm that. Thank you.

[*Translation*]

**The Chair:** As it now stands, we will not meet on December 13.

I also just wanted to say that the access to information commissioner tabled her report this morning. I just thought I'd let you know, in case you were interested.

Mr. Angus, you have the floor.

[*English*]

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

Will we have the Privacy Commissioner come one last time?

[*Translation*]

**The Chair:** Yes, next Tuesday.

**Mr. Charlie Angus:** Next Tuesday.

[*English*]

We are engaged in discussion about what we're going to do next. It's in camera so I'm not going to mention it here, but since I'm such a

nice guy, since Christmas is coming, I'm not going to carry this meeting on, because I can see you people just wanting to get out and get back home. I'm going to be reasonable tonight. I want that on the record. That's why I wanted it in public.

●(1715)

**Mr. Brad Butt:** I'm going to tweet that: Charlie Angus is reasonable.

[*Translation*]

**The Chair:** I have nothing else on the agenda.

[*English*]

**Mr. Charlie Angus:** I'm the nicest.

**Mr. Brad Butt:** I'm going to get all these responses back.

**Mr. Charlie Angus:** You're going to get all the trolls after you.

[*Translation*]

**The Chair:** The meeting is adjourned.

---







**MAIL  POSTE**

Canada Post Corporation / Société canadienne des postes

Postage paid

Port payé

**Lettermail**

**Poste-lettre**

**1782711  
Ottawa**

*If undelivered, return COVER ONLY to:*  
Publishing and Depository Services  
Public Works and Government Services Canada  
Ottawa, Ontario K1A 0S5

*En cas de non-livraison,  
retourner cette COUVERTURE SEULEMENT à :*  
Les Éditions et Services de dépôt  
Travaux publics et Services gouvernementaux Canada  
Ottawa (Ontario) K1A 0S5

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

### **SPEAKER'S PERMISSION**

Reproduction of the proceedings of the House of Commons and its Committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the *Copyright Act*. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a Committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the *Copyright Act*.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its Committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

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

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

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

### **PERMISSION DU PRÉSIDENT**

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la *Loi sur le droit d'auteur*. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la *Loi sur le droit d'auteur*.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

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

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