HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 051 • 1st SESSION • 41st PARLIAMENT

EVIDENCE

Thursday, October 18, 2012

Chair

Mr. Pierre-Luc Dusseault

Standing Committee on Access to Information, Privacy and Ethics

Thursday, October 18, 2012

● (1530)

[*Translation*]

The Chair (Mr. Pierre-Luc Dusseault (Sherbrooke, NDP)): Good afternoon, everyone.

Thank you for joining us, Mr. Lawford. You are our only witness today.

According to the agenda, we are going to spend about an hour on evidence and questions. We are going to start with a 10-minute presentation. Members will then be able to ask questions, as usual. Finally, during the second hour, we will go in camera for the debriefing on working sessions abroad.

Without further ado, I will give the floor to Mr. Lawford for 10 minutes.

Mr. John Lawford (Executive Director and General Counsel , Public Interest Advocacy Centre): Thank you, Mr. Chair.

[*English*]

I am here alone. Janet Lo, my co-counsel, sends her regrets. She's in a lock-up for CRTC on Bell-Astral.

The Public Interest Advocacy Centre is a non-profit organization that provides legal and research services on behalf of consumer interests, and in particular vulnerable consumer interests, concerning the provision of important public services. We have been deeply involved with the Personal Information Protection and Electronic Documents Act, PIPEDA, from a consumer perspective since its passage. We have published several recent reports: one on children's privacy online, one on a do-not-track list, and one on data breaches.

I've given the clerk a copy of references to those and summaries.

We're here today to talk about the immediate future of privacy. It is largely to be defined by services such as social networks. But social networks provide challenges to our concept of personal information and the commercial interests that are involved with that.

PIAC recently brought a complaint to the Office of the Privacy Commissioner of Canada under PIPEDA against Nexopia.com Inc., a social network based in Alberta and largely aimed at a teen audience. This real-life example illustrates the challenges of dealing with privacy and social networks, and unfortunately the inadequacies of PIPEDA to deal with improper privacy practices, even those where the improprieties involve children and teens.

PIAC alleged that Nexopia provided no comprehensible descriptions of the collection, use, and disclosure of the personal information of their largely underage users. We said that the company did not adequately detail its disclosure of information to advertisers, nor did it adequately detail how it used this information to serve up targeted teen ads. We complained that the default settings for personal information like gender, age, location, and pictures were open to the Internet—that is, not even closed to members of the site—and that this was unreasonable and even dangerous for the young users of the site. Finally, we noted that Nexopia appeared to keep personal information forever, even if an account were deleted.

The Privacy Commissioner upheld all our complaints. That was February 2012, some two years after we filed it.

Regarding default settings, the Privacy Commissioner wrote, in part:

> We do not consider making portions of a user's profile available to anyone on the Internet to be consistent with users' reasonable expectations, particularly when a user has clearly indicated his or her preference to share information on a more limited basis.

However, Nexopia has said to the Privacy Commissioner that they will not implement the four recommendations related to retention of data. The Privacy Commissioner has had to go to Federal Court to enforce her findings. Why?

First, the Privacy Commissioner has no order-making power. She has no fining power. Social networks that judge privacy findings too inconvenient or expensive, it appears, can continue to operate in a privacy-violating manner.

Second, the refusal reveals the real nature of social networks: they are financed by personal information. Asking a social network to destroy data appears to them like removing an asset from the balance sheet.

The Privacy Commissioner's trip to Federal Court will show if business purposes or the personal privacy of individuals is paramount under PIPEDA. However, the larger issue for you at this committee is how to help design laws to avoid this type of conflict from arising in the first place, particularly in the fast-moving social networking and online space.

Now I'll move to Bill C-12 and breach notification.

LinkedIn and eHarmony suffered large data breaches this spring. Social networks are now major targets of hackers, and there is a risk of exposure of personal information that is not intended for general viewing from these websites. This is in addition to the leaking of personal information from websites noted by the Privacy Commissioner at the end of September in a recent study.

Bill C-12 is intended to amend PIPEDA to provide for data breach notification. However, it does not succeed. It allows the company suffering the breach to make the determination of whether the breach is material enough to even report to the Privacy Commissioner. Part of that determination is an assessment, again made by the company of itself, of whether the cause of the breach or a pattern of breaches indicates a systemic problem.

● (1535)

It's extremely unlikely, in our view, that any company, but particularly a social network that trades in data, will declare that it has a systemic problem with data breaches and data handling that leads to breaches.

Bill C-12 is asking companies to declare that they, in effect, are negligent. As a result, we confidently predict that under Bill C-12 a social network or other online company will almost never notify the Privacy Commissioner of a breach that has not otherwise been made public. Companies are expected to determine whether to report data breaches directly to the consumers as well. They must determine if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual.

First, this threshold is very high. It's higher than U.S. state law requirements and it's unrealistic. It's difficult to predict how personal information will be misused.

Secondly, Bill C-12 ignores the blindingly obvious incentive for companies to find no such risk to individuals and avoid notification and its cost. As a result, we confidently predict that under Bill C-12, social networks and other online media companies will almost never notify individuals of a breach that has not otherwise been made public.

There is another model in Canada for data breach laws: the Alberta Personal Information Protection Act. In Alberta, all breaches must be reported to the Privacy Commissioner of Alberta, on pain of fines. The Alberta Privacy Commissioner then determines if the breach is serious enough to notify individuals on a test of potential for any harm.

PIAC studied public attitudes to data breach notification in focus groups in 2011. Overwhelmingly, participants preferred the Alberta-type model to leaving companies to make this decision. We urge this committee to express these concerns about breach notification under Bill C-12 in its report.

I will turn now to privacy policies. Social network privacy policies are “take it or leave it” contracts. The burden of determining what is done with personal information is borne by the user. Yet social networks regularly rely on the consent of users to justify practices and point to the use of the site as the equivalent of consent to the entire privacy policy.

It's PIAC's view that this legal fiction is in fact used in place of informed consent in many social networks. Users simply do not read all the policy, and if they do, they do not understand it. Why is this? This is because major social networks define “personal information” in confusing ways, and none of them define it in the way it is defined in PIPEDA.

Many define personal information as personally identifiable information, which, as you recognize, is a U.S. legal concept. Recently, many larger websites have dropped any definition at all of personal information, only to give examples of treatment of certain data elements like gender or age. The clerk also has a copy, which should have been distributed to you, of wording of privacy policies that we're talking about.

This non-definition of personal information matters because users reading the privacy policy are not able to understand their real rights under PIPEDA in order to launch a complaint or to bring the company into compliance or even to contact the company.

The Privacy Commissioner appeared before this committee and stated that social networking sites do not do a sufficient job of explaining their use of personal information. She said she doubts in these situations that the social networking site has real consent. We think the Privacy Commissioner is right. But the complaint mechanism under PIPEDA is very poor enforcement. She needs order-making and fining power.

PIAC suggests, however, that given the challenges of big data collection by social networking and other online businesses, this committee go further and consider a full enforcement framework such as that for the do-not-call list for companies flouting Canadian privacy law.

I'm going to close with some forward-thinking ideas on social networking and privacy.

First of all, there are many related entities dealing with personal information created at social networking sites in order to monetize that information through advertising and other methods. This committee should study these relationships and consider rules for revealing related parties in personal information trafficking akin to those rules in securities law to bring increased transparency to data flows in social networking sites and marketing companies.

Secondly, the committee should consider a national do-not-track list.

Thirdly, the committee should study the nexus between privacy and competition law, and whether the Competition Bureau actually has a role to play in addressing privacy concerns and where a merger or other practice can reduce competition. For many online markets, competition for eyeballs depends on the currency of personal information or the value of big data.

● (1540)

PIAC thanks the committee for this opportunity to speak. We are happy to answer questions

[*Translation*]

in both English and French.

Thank you.

The Chair: Thank you for your wonderful presentation, Mr. Lawford.

We will now move to the seven-minute question and answer period, starting with Mr. Angus.

[*English*]

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

Thank you, sir. This has been a very interesting discussion. If you've been following the course of our looking at the issue of social media, you'll know that we've been dealing with two major issues. One is the issue of not interfering with development, but ensuring that more vulnerable people—particularly young people—are not unfairly targeted, and that people's privacy is protected when it needs to be.

What we've heard from some of the main drivers on this new information highway is that they never speed, they always stop at the lights, they never do illegal left-hand turns, and there's no need to have police anywhere on any of this data-flow highway, and that things will just drive better.

I'm concerned that we have a case with Nexopia, which has breached the Privacy Commissioner's.... I think the Privacy Commissioner has found 24 breaches in Nexopia's handling of information. They haven't bothered to meet the deadlines set by the Privacy Commissioner; they're taking her to court to stand in the way of some of them.

Do you believe the Privacy Commissioner should have more tools to ensure compliance, so that we make sure that all the players in the market are following the rules?

Mr. John Lawford: We do, and the Nexopia complaint is a good illustration. But we could have chosen other social networking websites as well. The point is that we've gone through the process of identifying a site that seemed to not have made it clear to users what information would be used. The Privacy Commissioner upheld the complaint, and then they still didn't do anything. It may be that eventually Nexopia will follow the Privacy Commissioner's ruling, but it's a very inefficient way, I think, for her to go about it—especially since you see in Alberta and in B.C. and in Quebec that all those privacy commissioners can simply order a certain result.

It seems much more sensible and direct to have had, for example, the Privacy Commissioner's order made an order in February, and not to have to wait to see whether the company will comply. As far as the Privacy Commissioner is concerned, they're quite far offside.

Mr. Charlie Angus: We're not trying to damage the reputation of Nexopia, but their business model is focused on young people, and young people using the Internet should feel free, should feel that when they use it they're talking to their friends and are not dealing with trolls. Yet you seem to be telling us that Nexopia's business model is that anybody, at any time, anywhere can track who is on it, what school they go to, what their sex is, what their preferences are. Is their orientation or other things on there? Is that the kind of information that anybody can find out?

Mr. John Lawford: That's the core of our complaint. It was triggered by the fact that you can go on to Nexopia, and they even provide a handy-dandy database searching tool for outside users—or anyone—to search from the front page for age, gender, and the city where you live. And if you do that, you can also choose interests and target people, and you get real profiles. You get real profiles from the outside world.

They're also indexed on Google or any other major search sites, so you can put in “female, 13, Calgary, dancing” followed by “: nexopia.com” and pull up profiles from that source as well. We thought that was not exactly....

It's not the expectation of a 13-year-old who signs up. The expectation is that you're going to share your information with your friends, not be available to everyone on the entire Internet.

● (1545)

Mr. Charlie Angus: The Privacy Commissioner found the same. The Privacy Commissioner said that these rules did not meet the standards of the rights of protecting a vulnerable class in our population. Has Nexopia changed these settings?

Mr. John Lawford: They were asked to change their privacy policy and some other information on June 30, and they missed that deadline. They were asked to change their default settings by September 30 so that when you become a new member you are defaulted into “friends only”, and that this not be searchable outside of the site. They missed that deadline as well.

Mr. Charlie Angus: I'm concerned because I know they've taken the Privacy Commissioner to Federal Court on their refusal to delete data. All of us have been struck by the horror story, the Amanda Todd cyber-bullying case, and that heartbreaking line in which she says, "I can never get that photograph back. It's out there forever."

If a 15-year-old feels that they don't like what's happening on Nexopia or don't feel like they want to be part of it and they delete their account, the information is still being held by a commercial company. Are you saying that Nexopia has gone to court to be able to hold that data regardless of whether a young person wants it deleted or not?

Mr. John Lawford: No, I'm saying that when the Privacy Commissioner asked Nexopia to have a data retention policy and to provide users with a real delete key, if you will, they said no. And then the Privacy Commissioner thought it was important enough to go to Federal Court on her own to try to enforce her ruling, because she can't enforce rulings; she can only recommend.

Mr. Charlie Angus: Explain to us why it's important to have a delete button for young persons, or any person who decides they don't want to participate anymore. Maybe it's just getting a little too weird out there and they just want to have their lives back. Why should that option be very clear and very available?

Mr. John Lawford: We think that users and people.... It's almost a human right. You should have a chance to ask a company to remove the information. It's clear in the act that you are supposed to delete it if it's no longer used, so we don't see why you shouldn't have the right to remove it.

In Europe they're talking about a right to forget or a right to remove. It's a debate that's just starting in Canada. I think we should have it, because our group feels that it's a right of the user to delete the account.

Mr. Charlie Angus: These companies set up operations whereby young people can trade information and do all kinds of great things, but we need to ensure there are some basic rules that those companies play by so that bad actors don't come in and so that young people aren't exposed.

Are we placing undue responsibility on companies such as Nexopia to have privacy settings or to delete accounts when they're asked to delete them?

Mr. John Lawford: The Privacy Commissioner did a pretty good job of saying that even with the present act, these are the rules.

The trouble comes when the company says, "That's nice. Thank you for your finding. We'll continue to do business as we wish." The problem is in the enforcement. The act covers this. We won in 24 of 24 complaints. It's hard to say how you could improve the act. Perhaps certain tweaks would make it clearer. That's something the committee could study. For example, on data retention, it's not clear that the user has the right to delete. It just says, "have a data retention schedule". Maybe it should be made clearer.

Mr. Charlie Angus: Thank you very much.

[*Translation*]

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

I am now going to give the floor to Ms. Davidson for seven minutes.

[*English*]

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

And thanks, Mr. Lawford, for being with us this afternoon. We're certainly hearing very interesting statements from you.

I want to continue where Mr. Angus left off. You're talking about the fact that there could be certain tweaks to the act. You talked about data retention. Are there other things that you wanted to talk about concerning tweaks to the act?

● (1550)

Mr. John Lawford: It's interesting to stay slightly on that one as well. We haven't heard much in the committee—I've been watching it—about de-identification of personal information. That's used as an equivalent in the act. You can either de-identify or delete.

The research we've done in our paper tends to suggest some things never totally de-identify. Often they can be re-identified. So that would be a tweak. Perhaps we shouldn't have de-identification equated with deletion. Maybe they're different things.

Mrs. Patricia Davidson: I don't even know what de-identify is. We're all familiar with delete.

Is it another method people use to delete, or feel they're deleting?

Mr. John Lawford: Yes, and it's a very attractive model for some commercial uses. You can aggregate or de-identify and then use the information for other purposes: monitoring who comes to your site, what they buy, telling advertisers and your customers, and tweaking your site so that it works right. It has some good uses.

Just as with health information for secondary health purposes, you have to be very careful that the person's particular health record can't be linked back to him or her, even when you take out certain identifiers. It's a bit of an art to design that.

In terms of other tweaks for the act, the consent mechanism is the right way to go. The trouble we had with Nexopia and with our paper on youth on the use of social networks was that kids didn't understand the extent to which information would be used for other things once it was out there. Is there any sense, in this committee or otherwise, in talking about a different level of consent for certain ages?

In the States, as I think you've heard from Mr. Elder, there is an act whereby companies can't collect information on those under 13 years of age. I think that's a pretty good rule. But we haven't been having that conversation here in Canada. It's still possible to collect information on two-year-olds. It's likely offside, according to the Privacy Commissioner, but it's possible to take a swing at it.

Mrs. Patricia Davidson: Continuing on a bit more on the privacy policies, I think you described it as a take-it-or-leave-it policy with no informed consent. I think we've talked about this a whole lot at this committee, about the privacy and the consent forms. Nobody reads them, whether they're teenagers or adults. People just scroll down to the bottom and push "I accept" and away they go.

Do you think there is a way to standardize it and to make it understandable for the user?

Mr. John Lawford: One of the things I mentioned in my presentation was that companies define personal information in terms of the uses they're going to put it to for their own company. While that might be fine, a standard statement of what personal information is, according to the law of the jurisdiction they're working in, such as Canada, would probably be a good addition. That way the average user could compare. I know it's more language rather than less, but that's certainly a possibility.

We've also talked in a couple of papers about trying to produce easy-to-understand icons or shorter descriptions. For a website that shares personal information, you might have two hands handing over a document, that sort of thing. That's helpful, I think, for people who are time pressed. That might be one way to go. Definitely, getting people together and seeing if there's any common ground for standardization would also be a really smart move.

Mrs. Patricia Davidson: How would that be enforced? Would it be legislated? How would it be done?

Mr. John Lawford: Perhaps tweaking the act to say you have to state the act's own definition of personal information might be something you'd legislate. Otherwise, I think that would be something led by the Privacy Commissioner in a round table with stakeholders. It could be in the form of guidelines if it was going to come from the top down, but most likely it would be through the Privacy Commissioner and not through legislation. I see it as something that might be too difficult to legislate.

Mrs. Patricia Davidson: Is there a danger in legislating too much, because of the rapidity with which technology changes and the slowness with which legislation changes? Is it better not to have it in legislation?

Mr. John Lawford: Let's take the example of data breaches. Now there's something that has shown that, although we have a good act, something can come along such as hacking or data-handling practices that can become a chronic problem. It's worth tuning up the act for that. Otherwise, the act itself, PIPEDA, is very technology neutral and written in an all-encompassing way. It really just needs tweaks. It's not something that needs to be changed much. It's a good framework. What's missing on top, from our point of view, is teeth in the enforcement.

● (1555)

Mrs. Patricia Davidson: I want to go back for a minute to the issue you were talking about with Nexopia and the 24 concerns and complaints that were raised. I think they agreed to comply with 20, but not with four.

Mr. John Lawford: That's right.

Mrs. Patricia Davidson: Were those four all on retention issues, or were they on different things?

Mr. John Lawford: They were all on retention issues.

Mrs. Patricia Davidson: What would be different about them? Why would there be four different ones?

Mr. John Lawford: I believe one of them was a refusal to set up a retention schedule for new users. So it would say that you had to keep it for three years after you stopped being a user. One was offering a true delete button. There were two more that I'm afraid I'd have to take a look at my phone to find for you, but I could probably do that.

Mrs. Patricia Davidson: Is there a true delete button?

Mr. John Lawford: No. At the moment, Nexopia will suspend an account so that you can't get into it, but it is still in existence in their servers.

Mrs. Patricia Davidson: With other companies, is there is a true delete button?

Mr. John Lawford: There are not many companies that do true delete. My understanding is that you can go through Facebook for individual items and delete. But the question is whether they are truly deleted or not in backup of backup of backup. They say they are for most purposes. But you have to go item by item; you can't delete a whole profile easily. I don't know of any websites that do a good job of that at the moment, but I can't claim to know of them all.

Mrs. Patricia Davidson: Thank you very much.

[*Translation*]

The Chair: Your time is up.

I am going to give the floor to Mr. MacAulay, who is here with us today.

You have seven minutes.

[*English*]

Hon. Lawrence MacAulay (Cardigan, Lib.): Thank you, Mr. Chair.

I'm new at this committee. I appreciate your presentation and appreciate having you here.

Is there such a thing, even though Nexopia does not have it, as a true delete button? Can we know that information is not there?

Mr. John Lawford: I think that's a very hard one for social networks, which are designed to solicit and then keep information. That's the way they run. I don't believe they've been designed from the ground up to easily delete information permanently and to guarantee, on an auditable basis, that it's been done, whereas a hospital or something else that has a more robust data-handling information services background might be able to do that.

The problem they often cite is that they make backups. Then the backup has it. And then a previous backup has it, and you'll never get rid of it. So, theoretically, we can always get to it.

But it's just a system design thing. If it's required, then I'm sure they'll be able to design it into the next version.

Hon. Lawrence MacAulay: Again, perhaps it's inappropriate, but could it be designed? That's just a matter of opinion. I think the delete button is something like speaking to a reporter off the record: it's off the record till they need it. That's basically what you're telling us.

Mr. John Lawford: At the moment, I think that's the reality for most social networks, because the pressure is to keep data and/or at least anonymize it so it can be used for other purposes and you don't lose the value of it.

Hon. Lawrence MacAulay: It certainly seems quite serious to me when you can collect information on what sex they are, what they desire, and this type of thing. That's serious. They make money on this type of activity. It's totally unacceptable.

Mr. John Lawford: The Privacy Commissioner said in her finding, especially for youth users, that a lot of the information was sensitive: which school you go to, what gender you are. They had a very long list of interests, and a lot of the interests are things like clubbing, partying, drinking, or things that might be something they don't want parents or other adults to see.

Hon. Lawrence MacAulay: But they put it on.

Mr. John Lawford: It's a choice, so it's been identified by that person. There are also a lot of free forums, so you can write your friends, just like on Facebook or anything else. I think a lot of the information is just sensitive through its context.

Hon. Lawrence MacAulay: There's a big difference between being 14 and 24, too, and you don't want that on there.

● (1600)

Mr. John Lawford: A big part of our complaint was saying that it might be reasonable for an adult at 24 to make the choice to put that sort of sensitive information into a public area, but often teens don't have the maturity to understand that it's going to be available either outside the site, in the case of Nexopia, or even within the site.

Hon. Lawrence MacAulay: I take it you think the Privacy Commissioner should have more authority, more clout, to be able to enforce.

Mr. John Lawford: I'll just keep saying it: yes.

Hon. Lawrence MacAulay: What responsibility do the business websites and things like Facebook, Twitter, and Myspace have with regard to fully and transparently informing people exactly how and when their information will be used, or is it just a myth that it could ever happen? Does it ever happen, or is it like the reporter: when you need it, it's there, and you don't tell the people?

Mr. John Lawford: I think some websites of some commercial parties do a better job than others do. Google tries and tries. They're so big and complex I think they almost can't, by definition, make it clear. But we do find that when the sites try to write from the user perspective rather than from their business perspective, it comes out a lot clearer. If they're thinking what functions the person will be using on the site, it's often clearer to them than saying, "We may use it on an aggregate basis for these business purposes. We may give to our affiliates." And no one knows what an affiliate is, right? It's possible to do. It's a lot of work to have a proper privacy policy, but I think the responsibility is there on the companies, because they're getting personal information, it's what's driving the value of the thing, and their responsibility is to be clear.

Hon. Lawrence MacAulay: What relationship do social media sites have with data collectors?

Mr. John Lawford: There are a number of links between social media sites and data collectors. Nexopia, on the commercial half of their site, had relationships with marketers in which they claimed to have information on how teens thought and purchased, because of their data set. I'm quite sure that Facebook is using that. That's what they use to drive their IPO: we know what people want. That's fine within the limits of everybody knowing that they have that information and are using it consistent with what they said they could use it with.

Hon. Lawrence MacAulay: What direction is this heading in? Is it expanding farther? Should the government put more regulations in place?

Mr. John Lawford: I think there is a lot that is good in our act. It needs some tweaks. It's really a matter of having the Privacy Commissioner look into problem areas, because she's on it; she has the experts. She can be ahead of the curve and work with other privacy commissioners around the world to get on the hot spots.

It's not so much that we need to change the act, although maybe a data breach notification law that works would be helpful. It's not a matter of just piling on regulations.

Hon. Lawrence MacAulay: Thank you.

[*Translation*]

The Chair: Mr. Calkins, you have seven minutes.

[*English*]

Mr. Blaine Calkins (Wetaskiwin, CPC): Thanks, Chair and thank you, Mr. Lawford, for being here and for the role you play in protecting the public interest and consumer protection. It is a very critical role that you have.

I'm going to ask you some questions to try to flesh out some of these things. It's a very complicated thing.

I have the privilege of knowing your background as counsel and as a lawyer. My background—I used to be a database administrator and computer programmer, so I have a little bit of experience with this. I never built any information systems that dealt with social media, but I was responsible for large amounts of corporate data.

When you talked about the four things the Privacy Commissioner did, I think I blurted something out while you were saying it, and I apologize for that. You said the biggest corporate asset that a social media site has is the data. I can assure you that the net worth of an organization like Facebook isn't in the wires and cables and computers. There's millions of dollars of value there. There's billions of dollars worth of data, and that is the most strategic asset that any social media site would have. It's probably the most strategic asset that most corporations would actually have—their consumer, their client data—and of course there are a lot of laws and regulations pertaining to that, so it shouldn't be a surprise.

You also said that the Privacy Commissioner, in the first recommendations, had no order-making power and so on and had to go to the courts. I just wonder how you can, as a legal counsel, square the circle of coming before the committee and saying you want the Privacy Commissioner to be the investigator, the jury, and the judge, and have the entirety of the process, without any opportunity for oversight that a court would have, for example, the counterbalance.

I used to be a law enforcement officer too. I can say there are times I wished I was the judge and the jury and was able to administer the sentence, but all I could have was my role in charging the individuals and letting that judicial oversight happen. It happens for a very good reason.

So can you square that circle for me on why we wouldn't want some of the larger cases to have that kind of oversight?

● (1605)

Mr. John Lawford: I think I can. The way the act is structured right now is that the complainant or the Privacy Commissioner can go to Federal Court to enforce a fine. The company can't complain if it loses. That works fine if the first resolution is just an ombudsman-type resolution where we recommend that you change.

If it were to change to judge, jury, and executioner, where the commissioner fines or otherwise makes an order, then I think we do have to have the right of the company, obviously if it's a tribunal making the decision, to go to Federal Court and say “bad decision”. I think that would be a change to the act that would have to be made, because it's unfair otherwise, to have no right to appeal and you've been told that you are offside.

Mr. Blaine Calkins: Due process, absolutely.

Mr. John Lawford: I would agree, definitely, that that would have to be a change that would go along with giving order-making powers. For example, in Alberta it's very possible to go to Queen's Bench and say that a privacy commission decision was crazy and have it overturned.

If you want to separate the two functions, like you do with the Competition Bureau, with the commissioner saying “This is a bad practice”, and then the competition tribunal deciding if it really is offside, that is a lot of superstructure to add for privacy. It might be necessary on big cases. Maybe we are heading there, but I'm not sure yet.

Mr. Blaine Calkins: I appreciate that; that's helpful.

Moving on to the second thing, which I think there is some confusion on, there's been some discussion today about the whole notion of what “delete” means, what “deactivate” means. Deactivation does not mean deletion. For example, websites will ask you if you want to deactivate your account. A user might think they're deleting their account, but they're not. The information in the account still exists; it's just been deactivated. Some would say there are good reasons for keeping that information, because nobody else can start up an account that matches or mirrors the one you just deactivated. You would have two accounts that are the same. That might actually protect the interest of the particular consumer in certain cases, where nobody else can cyber squat. If the account were deleted, somebody could come in and easily do that.

For the most part, I understand the value in wanting some information deleted from a database. If I have information I don't want to have in the hands of somebody at a certain point, I think, realistically, I make an order or make a request of that particular organization to have that information deleted. I also understand the complexity of having multiple backups, whether they're static backups or dynamic backups. How do you go back to a static system and change it if you have to do a restore because you had a system crash? You're going to bring back information you might not be able to tag at certain checkpoints along the way in the recovery process.

This is a very complicated thing to do, not only from a legislative perspective but also from a technical perspective. Can you elaborate further on anything your organization has done, any counsel you can give the committee on what other jurisdictions may have been able to do to successfully satisfy some of these cases?

Mr. John Lawford: I would like to say I could just fill you in, but I know that because of the “right to forget” stuff going on in Europe, the Article 29 working party is working on this. I don't know what their technical committees are doing. It would be a very good idea to set up a committee, led by the Privacy Commissioner, with industry and other stakeholders, like consumer groups, to start doing the same thing here.

You're right; it is terribly difficult. There are other pieces attached to this that will be affected by it, and yet there seems to be a need and a want on the part of users to have certain things deletable.

I think we can do it, but it's not a matter of just passing a law saying you should get a delete button. I think it has to be done in combination with everyone or it won't work. It will be interesting to watch Europe, because they promote talking about it, but at the end of the day, they tend to pass laws, so we'll see.

● (1610)

Mr. Blaine Calkins: I don't know if you've been able to pay attention to conversations this committee has already had with witnesses. At the last committee meeting, there was an individual—I think it was Zushman—who said that with what we don't know.... I don't know what I don't know, and I don't know what the future technologies are going to be, even though I've worked in the information technology industry for a number of years.

We all know that social media is very good at posting pictures, photographs, other types of software. With the advance in biometric technology...we don't even know what future technology advancements are going to be capable of with information that's currently posted today. Some consumers might feel quite safe in posting information today, with today's known set of technology. Had they known what was maybe coming down the pike, they would maybe be less comfortable in posting a photograph of themselves today.

From that perspective, has your organization looked at any of the impacts of what's in store as far as consumer protection or public safety?

Mr. John Lawford: We did touch on it a little bit on the Nexopia complaint, because Nexopia requires, or it did require—I think it still does—that if you create a profile and you want to put a picture up, it has to be your face or torso. I don't know quite why torso is included, but face is. If you require people to put up a picture of their face, obviously we have the problem of facial recognition, which can be run over a network. This is a concern for us.

There's a situation where we might say the committee wants to think about recommending to Parliament that maybe you shouldn't be required to put up, at any time, a picture of yourself, your face, which could be facially recognized, if you don't want to—unless it's for a passport, that sort of thing.

It's an interesting area. It's one I'd like to explore more, but I'm afraid that's the limit of our work in that area.

[*Translation*]

The Chair: Thank you.

I will now give the floor to Ms. Borg for five minutes.

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

Mr. Lawford, thank you for joining us today.

You have done a great job of pointing to the commissioner's lack of power. As my colleague Mr. Calkins said, when Mr. Zushman launched a class action suit against Facebook, the commissioner had to turn to the court to solve the problem. If she needs to go to the court, perhaps she does not have enough power.

Some provinces allow their commissioner to impose fines, for example. Do you know how that model works in those provinces? Could it be applied here, at the federal level?

Mr. John Lawford: In Alberta, the commissioner can recommend a fine for data breaches. I have studied about 30 decisions like that, and they are effective enough to make companies change their practices when there are problems, even when the fine is $5,000 or $10,000.

If the commissioner has the power and the responsibility to impose fines, those decisions are tough enough for other companies to examine them. The commissioner's decisions are sort of small tests for data breaches that really benefit other companies, in the sense that it spares them from having to do the same thing. That is just one example among others.

Ms. Charmaine Borg: Thank you.

You talked about the investigation by the commissioner and her 24 recommendations regarding Nexopia. Correct me if I am wrong, but I believe that only four of them are presently in court.

What happened to the other 20? Has Nexopia followed the recommendations and the deadlines?

● (1615)

Mr. John Lawford: To date, Nexopia has not done anything, and the Privacy Commissioner of Canada has not said anything. I do not really know why the two deadlines of June 30 and September 30 have passed without anything being said. I would imagine that something is going on at Nexopia or that the company is taking some action, but we do not know why they are still not following the commissioner's recommendations.

Ms. Charmaine Borg: Thank you.

For some companies, it is about the business model. In your view, do companies whose business is data really want to apply what is currently being done to protect personal information?

Mr. John Lawford: It is difficult to answer that question. It does not have to do with the willingness or desire of companies to abide by the law; instead, it has to do with the fact that in situations, where the law is soft, it will be bent all the way. That's normal. It is done to do business effectively.

However, in the case of Nexopia, Facebook or CIPPIC, some people still have problems. In terms of Facebook, we have noticed that data breaches were connected to some applications. But the position of the company is to say that it is not responsible because third parties are involved. That problem has still not been solved, I believe.

To solve problems, the legislation basically has to be clarified and implemented.

Ms. Charmaine Borg: I am going to change the subject.

You indicated that data could be “de-identified” and subsequently “re-identified”. Can we come up with a potential solution to make sure that the data remains anonymous or that consumers can at least understand the process of “de-identification” and “re-identification”?

Mr. John Lawford: The committee heard from health care experts, and those questions have been examined with a fine-tooth comb, if I may say so.

In addition, should the Privacy Commissioner be invited again by this committee, you could ask her if any guidelines will be developed.

Ms. Charmaine Borg: Thank you.

The Chair: I am going to give Mr. Mayes the floor.

You have just over five minutes since you are the last person to ask questions.

[*English*]

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

Thank you, Mr. Lawford, for being here today and sharing your knowledge of this subject. You may find my questions a little simplistic, compared with those of my colleague, Mr. Calkins, who has a great knowledge of this.

In your opening statement you referred to the terms, "personal information" and "general information". Are those terms a challenge as far as identifying what they mean? Are the guidelines clear enough that discern what personal information and general information refer to?

● (1620)

Mr. John Lawford: I think they are. It's interesting, because Canada has this definition in PIPEDA of what is personal information, which everyone wants to avoid because it's so clear. It says personal information is information about an identifiable individual, anything about an identifiable individual. That's very wide. The Privacy Commissioner has made many, many decisions saying it's almost everything. It includes your net buy-offs on your computer. It includes your IP address in certain circumstances. It includes your hair colour, eye colour, what weight you are, everything.

A lot of the privacy policies, unfortunately, are drafted by American lawyers for American companies, and they do business in Canada. They have a different rule there—it's personally identifiable information—so they tend not to tailor it to Canada well enough.

Mr. Colin Mayes: One of the discussions we've had is the disclaimer of the terms and conditions when you enter into a site. It was interesting to me that you talked about a do-not-track list. I wondered if there would be the ability to put in an enforcement where they must have a data retention time, you have to agree to a data retention time, and have that right up there on the screen, first of all. Or make it a little bit simpler: sharing or marketing personal data, yes or no. Those kinds of things I think are very simple and people can understand, people like myself who are very simple when it comes to these types of uses. That's one area that I think can definitely be improved.

You talked about teeth in enforcement. The one thing about enforcement is that there's a cost to it. To do it properly, you need to have human resources as well as financial resources. Have you given any thought to where those costs should be borne? Should it be by the server, the taxpayer, or some regulatory body?

Mr. John Lawford: We've put a little bit of thought into that. That's why I mentioned at the end that the committee might want to look at the do-not-call or anti-spam model, where there are fees in the case of do not track, to buy the lists that you have to scrub against, and in the case of anti-spam, the fines go back to the CRTC to continue to do anti-spam enforcement. Now, one of those two models might help.

I want to back up, because enforcement to me—and I think this is the way the CRTC is doing it for do not call—is a pretty wide spectrum. They can start with notices, they can start with small fines, they can go and speak to trade associations. There are lots of ways before you have to go to the big hammer and the expensive overhead. I would hope that although it's a big nut to crack, it wouldn't be as expensive as something like do not track or do not call.

Mr. Colin Mayes: Would it be on a complaint basis, or would it be like an investigation whereby you monitor it?

Mr. John Lawford: It's the same as any other enforcement area, such as security. You'll take complaints and tips when you get them, but you have to have an arm out there doing enforcement on its own.

I think the Privacy Commissioner has done as much as she can with her budget. They haven't been very aggressive with auditing companies, which is one power they have. They haven't really self-started. That would be an area to encourage.

Mr. Colin Mayes: How do you reconcile personal information in the social media with things like credit checks and insurance companies collecting data on individuals?

If for some reason I don't pay my bill at a certain time and the company I am dealing with has aggressive credit collection and just throws that into my credit rating, which might be an AAA credit rating, and I don't know about it, that's data that might not be well founded and that I'm not aware of. How do you reconcile that with those types of applications?

Mr. John Lawford: It's interesting, because consumer reporting or credit reporting, which you're talking about, is something that pre-dated the privacy legislation. As you know, there are a few protections built into the provincial legislation. For example, you can correct information or you can at least put a note on your credit file saying that it is wrong.

When the privacy legislation was redone here in the late nineties, we said it wasn't a good enough model. That was a big part of what the committee working on PIPEDA talked about. That wasn't good enough. You have to give the person a right to actually demand to have information changed, and that is in the act.

You're right. The trick is in informing people that they have that right. Then how does that play out in a large, complicated organization so that it's quick and easy to do and fix?

I don't see that happening in social networks. It's not easy to take off one data element. It's not easy to fix one thing.

● (1625)

Mr. Colin Mayes: Personally, I think if a company is going to file a bad credit against your name, you should be notified. Not only do they send it out, but you are notified. Does that sound reasonable?

Mr. John Lawford: It does sound reasonable, and it also sounds sort of like what they're trying to do in Europe by giving users a little bit more control of information that is detrimental to them, by giving them more of a right to delete it or control it. Just saying that you have the right to have accurate data...well, who goes out and checks their data, as you point out? As well, some things are so sensitive that if it's wrong, it has consequences. I'm not quite sure how to fix that.

Mr. Colin Mayes: You might not know of that data from a creditor reporting to a credit agency.

Mr. John Lawford: No, and again, as far as social networks go, the only parallel is when you identify your data and it goes out to a third party, or the privacy policy says they can share with third parties and you didn't read it or didn't understand it and it goes out. It's sort of the same thing.

I think a social network would say that you put it in there and knew that it could have gone somewhere. It's not the same as credit reporting, where you don't know. But if you look at your credit application, of course, it says they're going to do that.

[*Translation*]

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

I understand that Mr. Boulerice has a quick question. So I am going to give him two minutes to ask it.

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

Thank you very much for joining us, Mr. Lawford. Your remarks were very interesting and relevant.

I have two questions for you. I would ask you to answer my first question with a yes or no answer. If there is a data breach, does the company itself decide to report the facts to the Privacy Commissioner of Canada? Is that correct?

Mr. John Lawford: For the time being, the answer is yes, according to the commissioner's guidelines.

Bill C-12 also provides for that, but it has not become law yet.

Mr. Alexandre Boulerice: In my view, that makes no sense. I am very reluctant to rely on self-regulation for those types of things. I find that a bit disturbing.

I will now sort of play the devil's advocate. My second question excludes children and teenagers. Most social media are essentially based on making private information public. As legislators, what do we do to protect people's personal information when the business model is based on sharing personal information?

Mr. John Lawford: Yes, that is the intent. In these meetings, you see the game the two parties play; those sites have a goal, and this legislation has another. For now, we are saying that the consent allows us to determine where to draw the line. The problem is that the conditions under which people give their consent are not clear enough.

The Chair: That brings us to the end of the evidence.

Thank you very much for coming here, Mr. Lawford.

We are going to suspend the meeting for a few minutes, since the next part of the meeting will be in camera.

Thank you once again.

As for the members of the committee, I will see you very soon.

[*Proceedings continue in camera*]

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