HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

# Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 020 • 2nd SESSION • 41st PARLIAMENT

**EVIDENCE**

## Thursday, May 1, 2014

---

## Chair

**Mr. Pat Martin**

# Standing Committee on Access to Information, Privacy and Ethics

**Thursday, May 1, 2014**

● (1145)

[*English*]

**The Chair (Mr. Pat Martin (Winnipeg Centre, NDP)):** Ladies and gentlemen, we'll convene our meeting, late as we are. We begin by apologizing to our witnesses. It was an unavoidable delay in that we had to conduct votes in the House of Commons.

We're here today as the Standing Committee on Access to Information, Privacy and Ethics to resume our study on the growing problem of identity theft and its economic impact.

We're pleased to welcome two witnesses, Mr. Avner Levin, an associate professor at Ryerson University, and Ms. Éloïse Gratton, a partner and co-chair in the privacy section of McMillan law firm in Montreal.

Welcome to both of you. We're going to invite you to make your statements, but we will have to truncate the round of questioning to one seven-minute round for each party. That should leave us time at the end of the meeting to conduct some committee business that we need to undertake.

We'll give the floor to you in whichever order you choose to proceed.

**Dr. Éloïse Gratton (Partner and Co-Chair, Privacy, McMillan LLP, As an Individual):** I will start. Thank you for the invitation.

[*Translation*]

I'll give the first part of my presentation in French and the second, in English.

I'd like to start by discussing the legal framework governing privacy protection and the response of business. Despite the legislation that exists, the Personal Information Protection and Electronic Documents Act, or PIPEDA, companies and organizations have no real incentive to comply with the act and implement appropriate security measures. What's the worst that could happen from a company's perspective? What are the risks if they don't comply with the act? Not much. The worst case scenario is that their reputation might be tarnished. For example, if a complaint is made, and at the end of the investigation, the commissioner decides to release the company's name, then obviously, the company's reputation might be sullied. That very seldom happens, though.

There is another potential risk. When an individual is notified by the commissioner that the act was in fact breached, that person can take the company to Federal Court for damages. The court has made a few such rulings in the past decade. In five to ten cases, the Federal Court awarded small amounts. In some cases, it awarded no damages, and in others, $5,000.

Last fall, in its ruling on Chitrakar v. Bell TV, the Federal Court awarded $20,000 in damages, and that was a first. Is this the beginning of a new trend? Perhaps. Only time will tell. One thing is for sure: not everyone has the means to take legal action against a company to obtain small amounts in damages. In privacy violation cases, the amounts often range between $5,000 and $10,000. Engaging in a court battle is a complicated and painstaking process.

Furthermore, at the federal level, no incentives exist with respect to class action lawsuits over privacy violations, which have the potential to improve compliance. Incentives do exist in other jurisdictions. And in many cases, companies comply with privacy legislation as a result. Just think of the recent security breaches. Last January, a security breach occurred at Human Resources and Skills Development Canada. In April, a security breach occurred at the Investment Industry Regulatory Organization of Canada, or IIROC. And class action suits were launched in relation to both of those breaches.

In the case of IIROC, a portable drive containing the financial information of 52,000 brokerage firm clients was lost. The damages sought were $1,000 per individual. That has the potential to motivate companies to comply, but under PIPEDA, that isn't an option. The legislation contains no such provision to motivate companies. And even if it did, a class action lawsuit isn't necessarily appealing because authorization to proceed isn't always granted.

In the Quebec case of Larose c. Banque Nationale du Canada, the Superior Court made a ruling in 2010. A typical breach, it involved a lost laptop containing the financial information of many clients. One of the clients was not very happy and took the National Bank to court. At the authorization stage, counsel for the complainant had to show that, as a result of the security breach on the bank's part, actual identity theft had occurred. The court stipulated that the fear of identity theft alone did not entitle someone to compensation. Had there been no evidence of actual identity theft, the court would not have granted authorization for a class action.

That tells you just how high the bar has been set. Proceedings of this nature are not straightforward. And the damages aren't very high. So what's left? If you can't seek compensation because you're afraid you were the victim of identity theft as a result of a security breach, there is little else you can do.

Let's come back to the legislation concerning security measures. Companies are advised to adopt security measures based on the level of sensitivity of the information. Even when companies contract out services to a third party, the legislation says they are still responsible for the information and must ensure its protection through the contract. In reality, what we often see is companies using cloud services or third-party contracts. They contract the service out and then turn a blind eye to what goes on.

● (1150)

I would like you to consider a provision in a piece of Quebec legislation that I see as very useful. It imposes an additional obligation on companies preparing to give or transfer personal information to a third party via a contract. I am referring to section 26 of An Act to Establish a Legal Framework for Information Technology. It reads as follows:

> Anyone who places a technology-based document in the custody of a service provider is required to inform the service provider beforehand as to the privacy protection required by the document according to the confidentiality of the information it contains, and as to the persons who are authorized to access the document.

The person who entrusts the function to a service provider and transfers the data to the provider, whether via cloud computing or some other means, has an obligation to tell the service provider how to protect the information in question. I think incorporating a similar provision in our legislation could be useful.

I am active in the protection of privacy and personal information. There is a prevention component to my work. That entails advisory services, compliance, training, policy development and so forth. I am also involved in crisis management. I help with the management of security breaches, provide assistance when complaints are made to privacy commissioners in various jurisdictions and give advice related to privacy class action lawsuits. Clients rarely ask me to do any prevention work for them unless they have had some sort of crisis first. That shows that companies aren't very tuned in to the issue. And yet, the legislation exists. Are they motivated to comply with the act? Not especially, because they wait until a security breach has occurred before taking action. Not until a crisis arises do they realize how costly it can be and that they might do well to invest in prevention.

It's also interesting to see just how many resources are being deployed to compliance and prevention around the coming into force of Canada's new anti-spam legislation. That piece of legislation is being taken seriously. It includes liability provisions that apply to administrators, executives and employers. And since the penalties it sets out are quite stiff, companies take it seriously. Ever since its coming into force was announced, the legislation has monopolized my practice almost full time. Is spam a bigger problem or greater evil than security breaches or identity theft? I doubt it. Why, then, is the situation the way it is? What are we waiting for to motivate companies to invest in prevention?

I have one last point. My second part will be very short.

Some studies show that most security breaches are the result of human error. I am referring to two studies, in particular, that were conducted two years after the requirement to report a security breach was imposed on companies. The first was done by Alberta in 2012-13 and lists all the notifications and security breaches. According to that report, human error was at fault in many of the cases. The second study was done by the Ponemon Institute in 2013 and says that in 33% of cases, employee error was to blame.

That, too, shows that companies aren't taking employee training around privacy protection seriously. Very often, the security breach resulted from a laptop being left in a car. Was the employee aware that behaviour posed a risk? Was a relevant policy in place? Was appropriate training available? The jury is out.

● (1155)

[*English*]

I know time is running. The second part is going to be quick.

I want to raise the fact that currently under PIPEDA we don't have mandatory breach notification, and I believe that this may well play an important role in addressing some of the financial harm that may be triggered in the case of identity theft following a security breach.

If individuals, whether they be consumers, employees, are notified, it will help them to better protect themselves against harm, such as identity theft, because once they're notified they're going to pay special attention to their financial statements every month, every day, tracking down any suspicious or unauthorized transactions. They're going to monitor their credit through credit-rating agencies, such as Equifax and TransUnion. It will also provide businesses with an incentive to establish better data security practices in the first place.

What's the status on mandatory breach notification outside of Canada? We have it in Europe and in the United States. Most of the states in the U.S. have breach notification laws. In Canada, Alberta so far is the only private sector jurisdiction that has this law, and they prescribe fines up to $100,000 for businesses. They have realized that this breach notification obligation in their law has increased the reporting of security breaches, and it has also increased the privacy training. Businesses are more inclined and are more motivated to spend, because they realize that it's going to be an obligation to disclose the breach if there is such a breach.

In Quebec there is a consensus that it is needed. In 2011, la Commission d'accès à l'information du Québec published a report in which they said that this is needed. It's a matter of time. It's in the hands right now of the legislature, but we will have also this obligation in Quebec shortly, hopefully.

At the federal level, we've had various bills that have been introduced: Bill C-29, BillC-12, Bill S-4 recently, and Bill C-475. The latest one is Bill S-4. Will Bill S-4 do the job if it becomes law? It's better than having nothing, that's for sure. Maybe it's not perfect, but it's better than having nothing.

I guess it would create the incentive for businesses to disclose, and I think we need to trigger that incentive. In an ideal situation there should be clear monetary penalties for not reporting security breaches to individuals and to the privacy commissioners. There should be a duty to report a breach as soon as possible. I'm cautious with providing fixed delays, because I've been on the other side. Sometimes there's a breach and you need to do the investigation before you start notifying individuals and privacy commissioners, because you need to know exactly what happened and what needs to be told or not told.

The Privacy Commissioner, I believe, should be given the power to order an organization to report a breach to customers. These orders should be made public and the organization should be named. I think that would create the necessary incentive for them to invest in preventive measures, which would be beneficial to address a financial harm resulting form identity theft.

This is my last point. It would not be a bad idea to have a uniform breach notification law in Canada. Various systems could become problematic when there's a breach. I know that a few years ago, the Uniform Law Conference of Canada drafted a breach notification act. Maybe it could be used as a tool.

Thank you. I think my time is up.

**The Chair:** Yes, Madame Gratton, but you made very good use of what little time you had. Thank you very much for a very useful testimony.

We'll go immediately to Mr. Levin, please. I should have pointed out that Mr. Levin is an assistant professor, but also the chair of the law and business department at the Ted Rogers School of Management, and director of the Privacy and Cyber Crime Institute at Ryerson University. That's a more thorough summary of your credentials.

The floor is yours, Mr. Levin.

● (1200)

**Prof. Avner Levin (Associate Professor, Ryerson University, As an Individual):** Yes, I have lots of hats to wear.

Thank you very much to committee members for inviting me as well. I apologize that my presentation will be completely in English. I don't have the skills in French like those of my colleague, so my apologies for that.

What I'd like to talk to you about today is the role of the banks in combatting identity theft and its increasing impact on the economy. I'd like to start with a recent study that my colleagues and I did on a growing industry that's called the financial aggregator industry and the risks that they pose. Then I'd like to talk very briefly about the role the banks play with the financial aggregator industry. Then I'd like to talk more generally about the banks and the role that the banks play.

Let me start with our research. This was research that was funded by the Office of the Privacy Commissioner of Canada's contribution program and it was led by a colleague from Sherbrooke University, Anastassios Gentzoglanis, so I want to give credit there.

The financial aggregator industry is an industry that pulls together for customers financial information from a variety of sources. If I have a credit card with one bank and a chequing account with another bank and a savings account with a third bank, the aggregator puts that all together in front of me, whether I'm doing that on my desktop, my iPad, or in some cases on my phone. We were curious in the research about the consumer attitudes with respect to that, as well as with respect to, more importantly, the security provisions that they have for the information that they take from customers, and the privacy concerns as well.

It's a growing market. There are seven operators that are operating right now in Canada. They're not Canadian necessarily. You may be familiar with some of the names, companies such as Mint, or some people may know Quicken. There's Check, which was once known as Pageonce. There's Yodlee. There's Mvelopes. There's a number of other companies. Our research proposed to talk to them in confidence without attributing anything to them, just to learn about how they work, what kind of security they offer, what safeguards they put in place, all the things that according to PIPEDA at the very least they should be able to provide. No one from that industry agreed to talk to us as academics about their provisions.

I would think that if they have good security and safety provisions for our financial information, they wouldn't hesitate to broadcast that. That would be a good news story for them. But not one in this industry agreed to talk to us. As they said to us, “There is no upside in it for us to talk to you.” We found that very, very concerning and troubling. From what we can surmise, there are about one and a half million people in Canada, and potentially more, who are using these services. We're talking about a younger crowd who's more interested in that as well and more open to vulnerabilities. That raises a number of questions with respect to this industry.

First of all, who regulates this industry? Is it the OFSI, the Office of the Superintendent of Financial Institutions? What's the role of FCAC, the Financial Consumer Agency? What about the Office of the Privacy Commissioner? Who do they report to? They're not Canadian businesses. They don't necessarily see the Canadian landscape as something that has anything to do with them.

I'll quickly talk about what role our banks are playing with respect to this specific industry. Our banks are telling us that the risk is entirely upon us as customers. They're treating it in their language as an authorized transaction, meaning it's the same as if I used my credit card for a purchase at a store or another vendor: I authorize that transaction, and therefore, if something goes wrong with it, that's my responsibility as a customer.

I think that's questionable as well, because I think the banks should be a lot more cautious in terms of this industry and a lot more protective of customers in terms of educating them, also just in terms of safety and security provisions, but the banks have taken the attitude so far with respect to financial aggregators that they want nothing to do with them. They see them somewhat as competition. Of course, each of the banks also has their mobile and desktop services by now. Some of them are interested in doing financial aggregation as well. I think between these cracks, consumers sort of fall. That's a problem with respect to this financial aggregator industry.

Let me talk at the end of my brief comments about the banks themselves. The question to be asked is, are the banks themselves any better with respect to identity theft and identity fraud and financial fraud that's related to the theft?

● (1205)

For several years now, my colleagues and I have been trying to get the banks themselves to provide us with information about identity theft and breaches that are related to identity theft. We have received no response. We asked the banks individually. We asked the banks collectively through the CBA, Canadian Bankers Association, which is their association, to provide information to us.

What we are interested in is exactly what would help the committee in its work. We would like to know the sources of fraud. Can you break it down for us by category, source, or origin? I'll give you some examples. How much originates in customers' and consumers' practices? For example, we just saw a story in the news the other day about easy passwords. What percentage of identity theft is because people have easy passwords or because people don't hide their personal identification number properly when they use it at a bank machine or a point of sale terminal? What percentage is because people are negligent and just carry it in their pocket or stick it on their forehead? We don't have the answers to this information.

Further, what percentage is because Canadian criminals are committing crimes, for example, by placing devices on ABMs, automatic banking machines, and stealing people's passwords that way? What percentage is by people using skimmers on point of sale terminals and stealing information like that? What percentage of crime would be characterized as petty and what percentage could be organized crime? What percentage is the result of rogue employees, whether they are working for a retailer or a bank? What percentage originates outside Canada in other countries where a lot of criminal activity originates, whether it's the United States, or some country in eastern Europe, or whether it's Russia, China, or another Asian country? As academics, how are we to know what to think about the reasons for identity theft and identity fraud? How is the Government of Canada and Parliament going to say this is the best policy going forward on these issues without having access to that information?

I would just like to be clear that we are not journalists, and we are not interested in attacking any specific bank. When we go to the banks we say that we are really interested in this anonymously and we're not going to attribute anything to any particular bank. We went to the CBA again and said to just give us the data as an aggregate, but as far we know, the banks don't even share that data with the CBA. We are forced to rely on whatever is put out there publicly, which to the best we know is old data from 2012. There is some information on the CBA website that makes no mention of these categories. Some information that goes back to mid-2013 was given by the Canadian Anti-Fraud Centre. That's the last data I saw, but it doesn't break it down by categories. It gives the overall numbers. It doesn't give a good road map for the future as to how you would like to proceed.

We know by talking to people informally that there are hundreds, if not thousands, of incidents that the banks characterize internally as problematic. I'm talking about thousands per bank on a yearly basis. What all these incidents are we don't know. Are they all serious? We don't know. Do they all involve identity theft? We don't know. Something about them triggered a response somewhere at the bank that says this is an incident that needs to be dealt with. As my colleague said, will they be breaches that will require notification to the commissioner or the consumers? We don't know. We have no good solid information about them or their impact on the economy or on us.

I should say that as part of our due diligence before coming in front of you, over the last couple of weeks we contacted all the banks again. As I said, this has been going on for several years. To date we have received no response to our requests from any of the banks or from the CBA. I think the banks have a key role to play here. They have to be transparent. They have to be accountable. As individual businesses they don't have to put themselves at any kind of disadvantage over their competitors in the banking industry, but as an industry group, it's part of what I would call their corporate responsibility to deal with this issue.

● (1210)

I urge you as a committee to call on the banks to share that information with the public and with academics, at the very least with committee members, so that you have in front of you the information you need in order to do the important work you've been engaged in.

With that, I'd like to thank everybody. I'd be happy to take questions, if we have time.

**The Chair:** Thank you very much, Mr. Levin.

The very questions you've put to us both strengthen our resolve and reaffirm our reasons for going into this study. I can assure you that the banks are scheduled as witnesses before this committee, and they will not blow us off the way they've clearly blown you off, I can assure you. We will use whatever authorities we have to make sure they answer those questions that are put to them.

We have time for only one round, sadly, and only a five-minute round. I can see that we will want to call both of you back as witnesses as we proceed with this study—I certainly hope the committee can agree to that—perhaps after we've heard from the banks again.

We'll begin questions with the official opposition.

Ms. Borg, you have five minutes, please.

[*Translation*]

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

Hearing what the witnesses had to say was indeed very insightful. I am going to fire off my questions as I don't have much time.

Two weeks after I began using Mint, my credit card was used fraudulently. I don't know if the two are connected. I may cancel my subscription.

You said there was a problem in that these companies aren't Canadian and therefore aren't subject to our laws. They still operate in Canada, however. What measures could our committee suggest to fix that problem?

**Dr. Éloïse Gratton:** They aren't subject to our laws, but even if they were, what incentive would they have to comply? That speaks to the first point I made in my presentation.

[*English*]

I don't know if you have anything to add.

**Prof. Avner Levin:** I do.

I would echo what my colleague has said. You need to have an effective regulator, one clear regulator, for these issues, and effective sanctions that the regulator could impose. The banks react quite differently to OSFI than they do to the Office of the Privacy Commissioner—no disrespect intended to any one of those—because of the powers that each institution has with respect to them. In order to be serious, I think we have to consider what powers we will give to whomever is decided to be the regulator.

We need one effective regulator, especially with all the smaller players as well. The banks are established businesses with traditions. The smaller players are also very concerning to me, because they're often not Canadian and they don't even know that they have Canadian law that they have to comply with sometimes.

[*Translation*]

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

I want to stay on the same topic.

The two of you talked about the fact that our legislation lacked teeth and therefore didn't do much in the way of consequences. And the commissioner has little authority to issue orders or impose monetary penalties.

Is Bill S-4 a good way to solve that problem? Is it missing certain elements? If so, what should it include to ensure we are well protected?

**Dr. Éloïse Gratton:** Towards the end of my presentation, I mentioned four or five points in that regard. But there is something else I would say.

In an ideal world, companies would be penalized for failing to report a security breach. The commissioner should have the power to issue orders and make them available to the public. When faced with the risk of a sullied reputation, companies—be they banks or telecom carriers—would be more motivated to report a security breach.

Of course, we could examine the bill in greater detail. For instance, is the real risk of significant harm test too high? Is it too subjective? Won't companies take the position that the risk is hard to measure in cases where data was simply lost, even if it is financial data?

How is it possible to measure the risk of misuse? That isn't always clear. Does the criterion give companies too much latitude? We could revisit that in greater detail, but it's better than nothing, to be sure.

**Ms. Charmaine Borg:** Mr. Levin, do you have anything you'd like to add?

[*English*]

**Prof. Avner Levin:** I think there's so much ink spilled by lawyers about what real and significant harm means that it sort of boggles the mind. I think the answer is that if you want to get serious, you have to give the commissioner the power to order businesses to do something. She's been asking for that. Other commissioners in the provinces have that.

So far, that's not in this current draft. I think it would be a wonderful suggestion and amendment to give more powers to the commissioner going forward with respect to the private sector.

● (1215)

[*Translation*]

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

That's precisely what I had proposed in Bill C-475, which I introduced and the Conservatives voted against. It's really too bad. We will keep trying to get similar measures passed.

Do I have any time left, Mr. Chair?

[*English*]

**The Chair:** You have about a minute and a half.

[*Translation*]

**Ms. Charmaine Borg:** Mr. Levin, I want to pick up on the lack of cooperation you mentioned. I found that very interesting.

Is there anything that could be done to encourage better cooperation between banks and academics? Why don't they want to cooperate? Is it possible that they don't have the data or that no experts are working on that kind of analysis?

[*English*]

**Prof. Avner Levin:** Perhaps I could answer that first.

I think it's exactly as they said there. They see no upside in it for them. This potentially reveals information about them that they'd rather not know. Academics love to criticize, and it's always sort of going back to that fear of some information coming out that they're not comfortable with. The banks in Canada have created a system for consumers where we don't actually feel the impact directly on our pockets most of the time, because once they agree that it's not authorized by us, they will cover whatever the fraud is.

If you do the calculations, that's not a huge cost to the bank. The banks have been saying two things. One, they say, “Leave us alone and you're not going to get hurt.” I think that has sort of been their dual message in all of this. The question is, is this going to suffice going forward, especially with talks in banks and other countries of raising some kind of limit of personal accountability? Some people have been talking about $50 being their personal responsibility if their account is compromised. I think these are very important questions going forward.

**The Chair:** I'm afraid, Mr. Levin, I have to cut you off there.

Charmaine, five minutes goes by very quickly. Thank you.

Next then, for the Conservatives, Laurie Hawn.

**Hon. Laurie Hawn (Edmonton Centre, CPC):** Thank you both for being here.

Mr. Levin, I'll start with you. I bank with TD, but I have a CIBC Visa. In both cases my debit card and my credit card have been stopped at various times. It was my fault because I forgot to tell them I was somewhere and it triggered whatever software they have that spots anomalies. While it's a pain in the neck at the time, I do appreciate it.

You talk about the banks, about the upside and downside and the bank saying there's no upside. If there's no upside, then there must be a downside for them. Do we look at penalizing the downside more? If I'm the chairman of the Royal Bank of Canada and I tell you that there's no upside to this, how do you respond to that? How do you tell what is the upside for the bank?

**Prof. Avner Levin:** Again, I don't want to really.... I think it wouldn't accomplish much for Canada if we attacked Royal, or TD, or CIBC.

I would say to them, as an industry, could you share with us what are the sources of identity theft and identity fraud? Where do you see the problem coming from? Is it an internal problem with your rogue employees? Fine, then we'll tell you that you have to do some things about it. But if it's another kind of problem, for example, is it my responsibility as a consumer? Is it all because I forgot to tell them I was going somewhere or not? We need to know where to sort of draw our responses, depending on that information. The problem that I have is that I don't have the information to give you an informed opinion on what's the best thing to do in terms of penalizing.

**Hon. Laurie Hawn:** Do you know if the banks share that among themselves? I mean, the upside, I would think, is their cooperating, because I'm sure they all have the same challenges.

**Prof. Avner Levin:** They have the same problem, but to the best of my knowledge they do not share it among themselves. They view it as a vulnerability, so they talk generally about the issues but they don't really share that information. As far as I know, they don't even share it anonymously with the CBA.

**Hon. Laurie Hawn:** It seems to me that would be an upside.

Ms. Gratton, we talked about the risk, the consequences, and the lack of planning. They wait until the crisis happens and then all of a sudden they run around with their hair on fire. If we increased the risk or increased the consequences, would that motivate them to be a little bit more serious about preplanning?

**Dr. Éloïse Gratton:** I believe so, and I think a great example is with CASL, the anti-spam law coming into force. People are taking it very seriously. The incentive is there if the penalties are there, and they have D and O liability, directors and officers liability, employers liability, so people are on board. So yes, I believe so.

**Hon. Laurie Hawn:** On the smaller claims side, class actions seem to be popular; obviously there's strength in numbers. Is that the best vehicle for these kinds of things? I think it's obviously an invitation for people to jump on the bandwagon.

**Dr. Éloïse Gratton:** Yes, a little bit. It's still difficult to be authorized, although in the last year we had two cases, one against Apple in Quebec that was authorized last summer. There also was one earlier involving the health law in Ontario, Kay, that was authorized.

They are authorized more and more, and there are more and more of them. At least it is creating the incentive.

I think it is interesting to look at the case involving Banque Nationale and LaRose, where the court said it would not authorize this case unless you proved you were a victim of identity theft following the security breach. How do you prove that? It's hard sometimes to make the link between the breach and the damages.

● (1220)

**Hon. Laurie Hawn:** Have you looked at any statistics about exactly that? How many people were actually victims, and how many people are simply jumping on the bandwagon because it seemed like a good idea at the time?

**Dr. Éloïse Gratton:** Well, in Quebec we have an opt-out system, so nobody is jumping on the wagon per se, but yes, you're right. There are lawyers who are making a living by filing privacy class actions, sometimes copycat files from the United States that they import here. In some cases we defend these cases; we act for the defence.

**Prof. Avner Levin:** If you look at the data put out by the RCMP or people who report fraud to the various organizations—and a year ago I think it was around $17 million in combined value—and you compare that to the combined value that the banks and the credit cards are reporting, which is around $440 million, then you can see the difference between what people are self-reporting and what the banks are feeling. Again, we don't know why there's that discrepancy, what the reasons are, and what caused all that fraud, if you will, beyond the $17 million, and where that comes from.

**Hon. Laurie Hawn:** What do you put more faith in: the stuff you get from the banks or the stuff you get from the RCMP?

**Prof. Avner Levin:** The RCMP are sort of saying that they think people just don't report it. If you ask them, they'll say that people just don't report it, that they are embarrassed, they're this, they're that, that it's not worth it, etc.

**Hon. Laurie Hawn:** Ms. Gratton, you talked about Quebec's section 26. It seems like common sense. How much responsibility is there on the transferee of the information to ensure that whoever receives the information understands completely their responsibilities for protection?

**Dr. Éloïse Gratton:** Well, it's a little grey, right? There's a contract. The contract is usually worded in very broad language saying that they need to protect the information in accordance with applicable laws.

They just want the business. They want the contract. They'll sign it. At the end of the day, what kind of encryption are they using? Where is the information going to be stored? All these facts are not necessarily taken into account, so I like this section from the Quebec law, which creates an additional obligation on the part of the transferor.

**Hon. Laurie Hawn:** That's right. I meant to say “transferor”, not “transferee”.

**The Chair:** Laurie, your time is up. Thank you very much.

Thank you, Ms. Gratton.

Now, from the Liberal Party, Scott Andrews.

**Mr. Scott Andrews (Avalon, Lib.):** Welcome, folks.

Ms. Gratton, early on in your testimony you talked about the Privacy Commissioner and enforcement powers. Could you give us some idea of what enforcement powers you think we should be giving her? Perhaps you could elaborate a little on fines and penalties and what would be some acceptable thresholds for her or the office to implement.

**Dr. Éloïse Gratton:** It should not be anything lower than what we have under CASL, right? Spam is an issue. Privacy and identify theft is also an issue, so in my view, why should it be any lower? If she had the power to issue fines for up to millions of dollars or hundreds of thousands of dollars, it would create, I believe, the incentive for businesses to take this law seriously.

Add in D and O liability and employer liability, and I think you have the full package.

**Mr. Scott Andrews:** You talked about businesses giving information to third parties. Could you elaborate a little further on that? Do you have any examples of where this goes wrong or at what point it goes wrong? Is it because the third party has the information and then when the contract is over doesn't dispose of it? Do you have any examples? Could you elaborate a little on that?

**Dr. Éloïse Gratton:** Yes. Sometimes it's not shredded. It's stored. Also, it's not digital shredding of electronics that are not.... The information is not erased. It's provided to another employee, another customer.... You've had the Staples case.

I had a case recently where the information got lost in transit. It was financial information. Who's responsible? Is it the courier company? At the end of the day, it's a little bit of everybody.... The company is responsible for the information that it provided the courier, but it's the courier that lost it. Why did it get lost? The waybill fell off.

You have a lot of different stories and different types of breaches. In many cases, as I said, it's human error. A laptop is left on top of a car or is forgotten at an airport. It's a lot of human error. There are all kinds and types of breaches, I would say.

● (1225)

**Mr. Scott Andrews:** In the case of most of it being human error, it's not malicious in intention, so how do you penalize for human error?

**Dr. Éloïse Gratton:** It's a good question. As for what they usually do, the first thing they look at is whether the organization had proper policies in place, and then, if they had these policies, whether the employees were aware of these policies. Had they received proper privacy training? Usually, if these two things have been addressed, if technical measures and policies were in place, and if employees were aware, you clearly limit the risk. It's not a perfect system where it's 100% bulletproof, but you clearly limit the risk.

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

Mr. Levin, I'd like to have a little chat about Mr. Hawn's point on the banks stopping our credit cards when we travel and that kind of thing. It's sort of an early warning system for identity theft when someone is using your cards without.... How do you think the banks are doing in that respect? Are they doing enough due diligence? Are they okay when it comes to that aspect? Do you have any research to show that actually they're very late and that by the time they get to this, a lot of damage has already been done?

**Prof. Avner Levin:** I don't want to be glib, but I have absolutely no idea. They refuse to share anything about their practices or their policies with academics. I would be speculating if I were to tell you that they're doing okay in terms of the algorithms they are running, in terms of the credit cards of legitimate people who went overseas and forgot to tell them and they stopped them. I can't say whether that was good or bad. We don't have information of how much fraud is occurring and why that fraud is occurring, due to all the other reasons.

We have a bottom line number. We said, for 2012, it was $440 million total combined that the banks and the credit cards had reported. We have absolutely no breakdown as to what the causes were and all the things they went through.

I am sorry, but I can't give you an informed opinion on how well they're doing.

**Mr. Scott Andrews:** With other witnesses we have talked about the credit rating agencies, and I think their testimony here is going to be important. They're the ones who can identify when this stuff goes on first.

Do you think the banks have a role to play in identifying when an identity theft has just started to occur? Do you think they have that ability, or is it that by the time someone goes to the financial institution it is too late to try to stop someone's identity from being stolen?

**Prof. Avner Levin:** I think they do have the ability. I don't think it has to just rest on the credit bureaus. I think they have the ability, because they are running those algorithms. Your credit card is declined if you forget to tell them. If they have what we call the false positives of stopping people, then they should have the ability of flagging the real fraud as it occurs and being a lot more responsive.

Everybody who has been through this with their bank knows that the banks are incredibly cagey with you. You often want to know where you went, what you did, what happened, what store it was. You will never get that information from your bank. They say that for security concerns, they don't want to—

**The Chair:** Mr. Levin, I'm afraid I have to cut you off there again.

Mr. Andrews, that concludes your time.

Our last questioner will be Pat Davidson, for the Conservatives, for five minutes.

**Mrs. Patricia Davidson (Sarnia—Lambton, CPC):** Thank you both for being here with us this afternoon. Some of the things we've heard are certainly enlightening.

Mr. Levin, can you outline for me what the main focus of the Privacy and Cyber Crime Institute is and its mandate?

**Prof. Avner Levin:** Yes.

Institute is a word that we use at the university to help a group of academics come together and conduct research on a variety of projects. Our mandate is in the two areas of privacy and cybercrime.

From time to time we have projects that have more to do with privacy, the protection of personal information. We have projects with respect to cybercrime. It depends on the individual faculty members who are affiliated with us and what they want to do. We have done projects in the past about privacy in the workplace, about privacy online and in social media, about online advertising, various issues faculty members are interested in researching. Our role is to support them administratively.

● (1230)

**Mrs. Patricia Davidson:** I'm interested to know the most likely causes of identity theft. Is most of it paper-based, or is it online and those types of things? Are you telling me that you can't tell us that today because you're unable to access that information?

**Prof. Avner Levin:** That's right. We've tried to launch research projects to investigate these questions exactly, and in order to do that we wanted to get access to the information from the banks. We were willing to sign whatever they required in terms of anonymity and confidentiality and all of those things.

Generally, as academics—as I said, we're not journalists and we're not on a fishing expedition—we share our reports with people who participate, so they will see that their perspective is fully and accurately reflected. We don't want to point fingers and blame. We give everybody the opportunity to comment if we're putting a draft report out. They may not like our conclusions, but they certainly have the opportunity to see that it's accurately reflected. However, we have been unable to get the banks to cooperate with us, or the financial aggregators that I mentioned earlier.

**Mrs. Patricia Davidson:** Would it be fair to say that you couldn't comment on who the primary victims are of identity theft? You have not been able to quantify how much of it results in identity fraud and those types of things.

**Prof. Avner Levin:** Exactly. I have not been able to do that.

**Mrs. Patricia Davidson:** Ms. Gratton, you talked about PIPEDA. In 2007, there was a fact sheet on businesses and identity theft that was published. The Office of the Privacy Commissioner noted, "Minimizing the identity theft risk means making the fundamental privacy principles enshrined"—under PIPEDA—"part of an organization's culture."

Do you think that organizations affected by identity theft have followed that recommendation?

**Dr. Éloïse Gratton:** Some do and some don't.

**Mrs. Patricia Davidson:** Has it made a difference, the ones that do?

**Dr. Éloïse Gratton:** Definitely, but at the same time, the ones that do follow the law are getting annoyed with the fact that others are not. Yesterday, a story came out about telcos disclosing personal information. I got a call from one of my clients saying, "Are we the only telco not disclosing personal information, because it's looking bad on our industry and we're following the law. It would be easier to just give out the personal information." So some are following and some are not.

**Mrs. Patricia Davidson:** If the information isn't there about who's affected by it, how do you quantify who is following it and who isn't? How do you determine that?

**Dr. Éloïse Gratton:** It's a challenge, but I think if we have breach notification, we'll know a little bit more. If you have one branch or one party collecting the information and collecting all these notifications to say that these are the types of breaches that are happening in the country, I think we'll have a better idea at least.

**Mrs. Patricia Davidson:** Are there particular measures that organizations could be taking to more efficiently prevent the fraud?

**Dr. Éloïse Gratton:** What I'm including more and more in the contracts are audit rights. It's one thing to say that you better protect the information, and it's another to have the right to go and audit the premises, the servers, how they're stored. I'm including these types of provisions more and more in contracts, cloud services contracts. It's one way to do it.

**The Chair:** Pat, I have to interrupt you. We're at the five-minute mark.

That concludes the time we have set aside for questions. I'm truly sorry to have to shut this off, because we're fortunate to have two such leading authorities as yourselves come and share your testimony with us.

We value it very much and we will benefit from it very much. I hope we have the opportunity to hear from you again, should the committee members feel it advisable after we've heard testimony from the credit agencies and the banks.

Thank you so much, both of you, for being with us today.

We're going to suspend the meeting briefly while our witnesses leave the room, and we'll reconvene in camera for the study of future business.

[*Proceedings continue in camera*]