HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 033 • 2nd SESSION • 41st PARLIAMENT

EVIDENCE

Monday, February 23, 2015

Chair

Mr. Pierre-Luc Dusseault

Standing Committee on Access to Information, Privacy and Ethics

Monday, February 23, 2015

● (1530)

[*Translation*]

The Chair (Mr. Pierre-Luc Dusseault (Sherbrooke, NDP)): Good afternoon, everyone, and welcome to the 33rd meeting of the Standing Committee on Access to Information, Privacy and Ethics. We are continuing our study on the growing problem of identity theft and its economic impact.

A few months ago, several witnesses appeared before us to address this very important issue. We will now hear from two witnesses who will talk about this issue. Each witness will have 10 minutes for the presentation. Members of the committee will then be able to ask them questions.

We will first hear from Ms. Sherbanowski, executive director of the Crime Prevention Association of Toronto. She is joining us live by videoconference. Then, I will give the floor to a guest who will speak live from Orlando, Florida: Claudiu Popa, chief executive officer of Informatica Corporation.

My thanks to our two witnesses for their time today.

Ms. Sherbanowski, you have the floor for a maximum of 10 minutes.

[*English*]

Ms. Janet Sherbanowski (Executive Director, Crime Prevention Association of Toronto): Thank you for the opportunity to appear before the committee.

The Crime Prevention Association has been working with consumers and with government at various levels for over 30 years. We look upon our duties as mainly protecting the interests of individuals and the public. We do work a great deal with corporations and the private sector, but it's mainly on working with consumer groups and with individuals who have come into contact with people who perhaps may have stolen their identity or used their identity, or with whom they are concerned that their identity might be at risk.

Just to give you an overview, this is our third year coming up for working with the Competition Bureau and with a group in Toronto, with the Toronto Police Services Board, on fraud and related issues.

On March 20 we have an annual day called change your PIN day. We use this as a spring into action to get people to think about changing their PIN, their personal identification number. This is a very difficult thing for people to actually do because everybody has it memorized as their dog's name or their mother's birthday or their grandmother's year of birth. So we suggest each year that people put the year after it, for instance if it was 1886 you would use 18865 for this year. It's a very popular thing and it has been picked up by other crime prevention related groups across the country. We're very proud of ourselves to have become involved with that and provided a way for people to think about their identity.

As I said, we also work with the Competition Bureau. We participate with the federal group each year.

We've worked with New Horizons for Seniors, where we've done workshops for both new immigrants and seniors. As we've progressed, we've also done those kinds of workshops with the Ontario government, working with new immigrant and youth groups to help them understand about credit and identity fraud and the various risks in Canada.

We've worked with the Royal Bank and also with Scotiabank, which sponsored the ABCs of Fraud for a number of years and provided funding across Canada for that group, which in 2011 lost its funding. We've been doing it as a volunteer group for the last four years.

We work with a number of people on things like romance scams, mortgage frauds, condo purchases, and fake marriages. On the same day that I received the invitation to come to this group, I received an e-mail from a lady. In a growing number of cases we're looking at job-related scams and fraudulent use of information and identity. The lady sent me an e-mail, which I will share with the committee. She had put in a job application for a Service Canada position, which as a government position any information sent for this should be going strictly through the government. What happened is that she received an e-mail back from a group that is actually a travel agency, which arranges religious pilgrimages. They were requesting that she provide references and a police record check. The lady in question sent me an e-mail asking what our opinion was on this. I told her we would be forwarding the information to the RCMP on her behalf with her permission, because this is the type of information that can in a growing way be used, not necessarily financially against this woman, but her identity perhaps could be used to create an identity for someone who could be involved in terrorist activities.

A number of issues are arising even among the consumer industry where people's identity can be used without their knowing it. The more we look at it, where information is sent by e-mail on growing unemployment issues, we can see it's very easy for someone to take that information and create a fake identity.

● (1535)

In a number of cases they have the social security number. They have the whole history of where the person has lived, where they got their education, every job they've had. In this case, when someone is requesting information from them—references and a police record check—this degree of information provides people an opportunity to create a very good profile, and to commit not only financial fraud with their information but also perhaps something far more nefarious when we look at other issues.

In Ontario, CPAT worked with the Privacy Commissioner to find out what information we could provide to consumers about protecting their identity and how we could relay to them that there is a risk with big data and with the way data is being mined by corporations and perhaps government, so that consumers could be aware that, when they are asked for information beyond biographical details or beyond a level they are confident in giving, they can ask what they should be giving and where this information is going to be used.

From our perspective, perhaps consumers should be warned when financial institutions, for instance, in a criminal fashion under-report breaches or thefts of data on credit cards or debit cards. Such under-reporting does not give us an opportunity to have our policing beefed up and perhaps to hire more people in police services or government services to look at these issues. We've looked at a number of these issues with regard to trying to protect consumers whose trust in our ability to protect them and their information is being eroded. People whose trust is eroded do not feel that their interests are being properly met by government services or other service providers, and, in the case of this lady who sent me the e-mail about her information, even when they go to apply for a job.

One of the other aspects, certainly, is the retail industry's mining of data to find information in order to, for instance, send you a pair of shoes, which you then have to send back. You're being caught up in what we used to see many years ago with book clubs. You're being sent all of these products, because you have opted for one type of service and you are being exposed to and perhaps charged for a lot of other services you aren't aware you're also opting in for.

I belong to several different groups that look at data. Today I received a request from a group to evaluate a program that a research company will offer to schools. The program will ask teachers or school boards to track activity among children. This information, in my opinion, will also be used by insurance companies or financial institutions or health IMOs to track whether people will be eligible for health-related products in the future. If you take somebody in grade 1 or kindergarten and you're tracking their physical health activity through until grade 12 with this type of new app, then an IMO 20 years from now could say, “Well, you didn't participate in enough sports, so you're not going to be eligible for a diabetes program”.

● (1540)

So, if we are looking at it now, there are a number of issues beyond identity theft that become identity usage. With regard to privacy, big data collection, and the use of data, we have an opportunity at this point in our history and development to perhaps create a robust risk assessment for consumers.

That's it. Thank you.

[*Translation*]

The Chair: Thank you very much for your presentation.

Without further ado, I will give the floor to Mr. Popa, chief executive officer of Informatica Corporation, a company that provides data integration software and services. He is joining us by teleconference. I thank him for his participation. His experience will help us address this growing problem of identity theft.

Mr. Popa.

[*English*]

Mr. Claudiu Popa (Chief Executive Officer, Informatica Corporation, As an Individual): Thank you again for the opportunity. I appreciate being invited.

My name is Claudiu Popa. I own a risk management consultancy in Toronto. We're focused on security and privacy consulting.

We operate nationally across most sectors. We audit globally. We provide risk assessment services of a privacy and security nature, as well as business continuity and disaster recovery. We test the standardization of protective approaches and practices within both private sector and public sector organizations, so we have a certain privileged outlook and visibility into what organizations do. Of course, we aggregate some of that just for the purpose of having our own insight into our own industry.

All our engagements and clients are, by default, confidential. We look at what trends we can identify and conduct research. We publish white papers. We publish books. We hold seminars and educational events to share some of that information.

One of my latest books, one that's being published this year, is focused on cyberfraud and cyberfraud taxonomy, which I feel is sorely needed around the world.

From the perspective of a cyberfraud being a global concern, we are noticing massive trends making their way around the world in many cases, and in most cases before they even hit Canada, so there is a predictive element to this we try to identify in the publication.

We are seeing global trends of any number of types, but we're seeing very little in the way of shared taxonomies and shared definition, especially when it comes to law enforcement collaborating.

We do know from an identity theft perspective the issue is growing, but more importantly, we feel that it's morphing, and so our research is showing that as we track the types of breaches, I'll say, around the world, every year we are seeing a lot of innovation in a negative way, of course, as to how this type of crime is evolving.

We have all seen the kinds of studies that have been published by Intel and McAfee in their 2014 global cybercrime report, which shows that up to $575 billion in annual value is lost due to cybercrime, a lot of which—and according to the breach level index for last year, most of which—is arising from the billion-plus individual records that have been compromised, and that was just for last year.

We see the damage is certainly not limited to Canada. It's global. We're also the first ones to identify the impact on individuals, and that's who ultimately get hurt because these are innocent people. Of course in many instances their personal information was entrusted to information custodians that may or may not have the right protective controls in place.

The FEC for example, the FBI, and certainly Canadian sources have cited it takes at least six months and 200 hours, and I've seen estimates of up to 800 hours, to recover identities once they have been damaged by these kinds of breaches. In many cases it happens to people who do not have the time and resources to deal with these kinds of situations. It's a terribly unfortunate and evolving type of crime that victimizes not just the most independent people in society, but in fact, the most vulnerable.

One of the things I wanted to establish was the difference between personal data breaches, the types of information that is being lost when there is a security breach that we see in the news, the terms “identity theft” and of course “identity fraud”. I think it's important to define these things adequately or at least treat them differently.

● (1545)

I am not going to serve as *Webster's* today, but I just want to make sure that we differentiate between their uses because, as they evolve and as we see emerging trends develop, these things are taking on very specific behaviours that we can and should be tracking. In fact, for the purpose of predicting some of their evolution, it's important to do.

We're seeing an explosion in social engineering use. Certainly, phishing—and spear-phishing—is one of the practices that's most commonly used to break into organizations, gain access to personal computers, install software without authorization, and things of that nature. The reason these are particularly effective and damaging is that they are addressing victims individually using any kind of information they can get their hands on.

This targeted information has a lot to do with the click-through rate and the rate at which e-mails are being opened as the result of receiving a targeted e-mail. If I receive a targeted e-mail from CIBC, let's say, that calls me by name and tells me there is some issue with my account, I'm a lot more likely to click through, especially if I'm not well versed in proper security practices.

More importantly, there is a lack of standardization in the practices of Canadian organizations when it comes to including active website links in e-mails that they use to communicate with the public. These are organizations that should know better in many cases, and we often write about that.

We do see that part of the threat is due to the quasi-legitimacy of misleading organizations, such as, for example, organizations that pop up a window on a screen and say that there is an infection on a computer. Of course, they've gone in and infected the computer first and are claiming that there's an infection, but in addition to that, there is a price to be paid for disinfecting the computer. Now, some of that disinfection is real, but most of it is not.

The way to catch these organizations may not be to place them in the same box as criminal companies, because it will be very hard to prosecute them if in fact they are providing a legitimate service, supposedly. That's a very difficult thing to do, because we found that for a lot of these organizations, even if they do not infect the computer or use spyware or things that are eventually traced right back to normal advertising practices in some cases, in many cases these guys even have support departments, and they provide refunds without any questions asked. It's very difficult to put in place the legislation that would protect these guys from acquiring personal information, abusing it, reselling it, and participating in this cycle of cybercrime.

We know that a lot of this type of victim targeting includes individual calls, not just e-mails. It's very difficult for recipients to say no. In many cases, they are pressured, and there are repeated calls to these individuals using particular information. I've received some myself asking for social insurance numbers and driver's licences, and they are very insistent. It's very difficult for regular individuals not just to be aware that these things are happening, but to enforce a personal policy to not share some of this personal information.

The global scale is what we care about. On a global scale, we see that data theft is happening on a massive level, and personal data theft is what I mean. It participates in things as significant as human trafficking and funding terror. We are now able to track this type of thing. We're not able to quantify it precisely, just like we're not able to precisely quantify cybercrime, but we can see where the money is going.

● (1550)

If we had more collaboration from law enforcement, particularly the way it's done in Europe...Europol, for example, and Interpol are having tremendous success on a sector-by-sector basis.

We are also seeing the ineffective use of credit brokerage firm services as a knee-jerk reaction to breaches. Whenever there's a massive breach, immediately the organization that has fallen victim to them is offering free credit and identity monitoring to all victims, and that's it. We find this is insufficient. In many cases these organizations, in their own practices, do not conform to standard best practices for anti-phishing or identity protection. They do not even follow secure development practices for some of the tools they offer. For all intents and purposes, these are very weak controls and the standardization of these safeguards should be revisited.

We obviously need to establish rules against predatory practices. As I said, organizations should not be allowed to victimize individuals and to call them time and time again, or certainly to lure them even with services they are prepared to provide refunds for, because that's not how their business models work. Their business models work based on the personal information they steal, and the money that is exchanged is gravy for them. They actually monetize the personal information and the personal details of the victim. So that's a big deal.

We do need to create stiffer penalties for complicity within cyberfraud, but we do need to establish measures to determine *mens rea*, for example, for many individuals who fall prey to the promise of profits without actually being part of the organized criminal element. In many cases they see an opportunity to make money, and they think it's a regular job, and then they go to jail for it. That's seen as an issue.

I'll just wrap up. We need a standardized understanding of acceptability regarding the requirement for social insurance numbers, the collection of driver's licence numbers, and the risks associated with doing those things, and of course, we need to have real practices around not just privacy but also the use of big data. We're going to identify things like synthetic identity theft and identity fraud within the realm of what we are now calling synthetic ID by using big data analytics. We are going to require the banks and the insurance companies to collaborate so that we can identify risk trends and build models that allow us to identify these guys. Right now there are people in Canada and around the world who just walk the street day in, day out and manage dozens, if not hundreds, of identities not just for existing individuals, but for fictional individuals. That's another reason why the credit bureaus are not effective in catching these guys, and a lot of these synthetic IDs are still damaging the identities of the victims from whom they may have borrowed only one ID element to combine with those of others and create a fictional individual that they use to create an economic or financial windfall for themselves.

That's what I have to say so far. Thank you for the opportunity.

● (1555)

[*Translation*]

The Chair: Thank you.

I have to interrupt you because you are a little over your speaking time and to allow members of the committee here today to ask you questions.

Let’s move right away to the first round of seven minutes. Let me remind the members of the committee to indicate whom the question is for before asking it. In this way, the witnesses joining us by teleconference or by videoconference will find it easier to know whether the question is for them or not.

Ms. Borg has the floor first, for seven minutes.

Ms. Charmaine Borg (Terrebonne—Blainville, NDP): Good afternoon.

First, I would like to thank our two witnesses. The two presentations were very interesting.

Mr. Popa, my first question is for you. Your organization is not based in Canada. I am particularly intrigued by the fact that your organization is international.

What stage are the Canadian organizations at in dealing with privacy? Are there improvements to be made? Is Canada a leader in the field? Based on your observations, where is Canada at internationally?

[*English*]

Mr. Claudiu Popa: I happen to be in Florida on vacation. I am based in Toronto and live in Toronto; however, I can still answer that question. That's why I didn't interrupt you.

[*Translation*]

Ms. Charmaine Borg: I apologize.

[*English*]

Mr. Claudiu Popa: It is my job to keep an eye on how legislation is effectively assisting with combatting cybercrime around the world. Because we're advising at the board level, we need to have that kind of visibility across not just sectors, but borders.

What we're finding is that the rumours are true: Canada's privacy legislation and Australia's for the most part are very innovative and very effective in and of themselves; however, they're not being used effectively. We're finding that organizations as a whole—not law enforcement, but businesses—are not embracing and not internally enforcing proper practices for at least two tenets of privacy, or at least of fair information practices. Those are the collection and the safeguarding of information. A third would be the disposal, which is sorely lacking. We're seeing this across borders.

We are seeing a lot of proper enforcement down south in the U.S., because there are stiff financial penalties for it, and they fall under security legislation. However, for Canada, which doesn't have much in the way of security legislation, privacy legislation, if correctly applied, could serve to benefit the public and protect it from identity fraud simply through the enforcing of those three tenets of fair information practices.

I'm not sure whether that answers your question, but this is what we're seeing.

● (1600)

[*Translation*]

Ms. Charmaine Borg: Thank you very much. That fully answers my question.

Let me apologize for assuming that you were American when you are on vacation down there. In fact, we are very jealous of your trip in a warm place.

Here is my second question. Please correct me if I misunderstood your remarks.

You said that, when there is a breach of privacy within an organization, the organization often says that it will follow up on the credit file in question. You seemed to be saying that this is not sufficient. If that’s the case, what are you proposing? How should we respond when a breach of data could lead to identity theft?

[*English*]

Mr. Claudiu Popa: That's an excellent question.

We're finding that the most meaningful research we're doing is at the enterprise level. It accounts for the vast majority of personal information breaches, and for the breaches that are in the tens or even hundreds of millions of victims. So in looking at how large organizations are handling data breaches, we're finding it entirely inadequate because there is a huge machine that kicks in. As soon as there's a breach, there's a huge communication security component that kicks in, and it has everything to do with reputation management. For reputation management protection, they immediately kick in. Obviously, they'll work with law enforcement, but they don't do it quickly enough.

For example, in Canadian privacy law there's always that written expectation that you need to be right on top of things and start sharing and documenting information right away. We're finding that enterprises are sometimes taking a month or two to report breaches. By that time, of course, the victims have already seen their information copied, re-copied, resold, and repackaged many times, and that's a big issue.

But the bigger issue that we're seeing is in the inadequacy of that response, which has to do with simply taking part in this reactive way of engaging with the credit bureaus and saying, “Okay, how much is this going to cost us on a per record basis? We lost 10 million records. What will it cost us?” They engage with TransUnion or Equifax, and they offer this service free for one year. This free service for one year simply gives people access to a dashboard and sends an e-mail when a breach is detected by the system. I've never met anyone who received a meaningful message regarding their identity data. I have met a few people who have received meaningful messages when it comes to their credit rating changes, but there's very little assistance as to what happens next. So it tends to be a measure that is entirely inadequate as far as we're concerned.

As far as what would be adequate is concerned, first, we need to have some legislated expectation as to the number of days that organizations need to allow before they contact law enforcement. Our preference is that they already have a relationship at least with privacy commissioners, and they have the right practices in place and the right privacy impact assessments conducted so that these can right away be examined and analyzed by law enforcement and by commissioners as soon as a breach is detected.

The lack of breach notification in Canada is a major drawback, at least on an international scale, let's say, compared with the U.S., where breach notification is legislated. Here in Canada we don't have that, except in certain sectors, such as health care in western Canada, but it's not pervasive. So it's poorly understood and it has been very much pushed back, simply because as soon as you say “breach notification requirement”, it automatically means that every organization needs to invest actual money in detective controls, in the ability to detect breaches. Without the ability to detect breaches, they don't have to be necessarily responsible for these things because they can claim ignorance. But once they detect them, they have to do something about them.

My big thing is to legislate breach notification and that will protect the public.

● (1605)

[*Translation*]

The Chair: Thank you.

Ms. Borg's time is up.

I now give the floor to Ms. Davidson, for seven minutes as well.

[*English*]

Mrs. Patricia Davidson (Sarnia—Lambton, CPC): Thanks very much to both of our presenters today. It's a very interesting topic. Although we started getting this under way many months ago, I think the technology and the situation itself is evolving so quickly that every time we hear presenters, we hear something new.

That brings me to my first question, which is for Ms. Sherbanowski, please.

Could you give us what you see as the definition of the identity theft issue in Canada, and how it has evolved, and I don't want to say “over the past decade”, because I don't think we have enough time to talk about how it has evolved over the past decade, but how has it evolved over the recent past?

When you're talking about that, what are the most likely causes of identity theft? Perhaps you could bring into your answer how much of that identity theft is paper-based, whether it comes from mail, credit cards, or passports, or how much of it you think occurs online.

Ms. Janet Sherbanowski: In terms of the ABCs of Fraud group that we were working on with consumers, in its evolution I got to see all of the information that had been prepared. It went right from the little skits they had done 10 years ago that were very vaudevillian, that were telling people about somebody telephoning with a granny scam and things like this.

The evolution has been very sophisticated, and that has been one of the difficulties: Who do you protect? There are our most vulnerable seniors, who are still paper-based to a great extent; the more sophisticated seniors, like me, who use the computer for all of our banking, e-mail, and everything; and the youngest members of our society, who now have cellphones and are texting back and forth at the speed of light. The evolution of your identity is as fast as light right now, and the people who I think are most vulnerable with this are the kids. I see their use of technology and the appreciation of that communication, the constant ongoing communication, as being very, very dangerous.

My grandson is 12 years old. He called because he wanted to buy something new online that was $3.24. I went and looked at this, and I said, “Wow, you have a lot of information there on yourself.” A 12-year-old is now far more sophisticated in giving out information than would be someone who's perhaps 60. The level and the evolution of that depends on the age group we're looking at. I think the most vulnerable now are the youth, in both the sexuality identity and the use of their faces on sexual images.

Your identity is a vast conglomeration now. It isn't just giving out your SIN, PIN, or driver's licence number. It can be something that becomes one of the animes. You've gone into a game and you've created an identity. That identity now becomes something that is very real in cyberspace—saleable, trackable, and minable. These identity things go from paper-based, which is still being used, to very sophisticated gaming technologies to Bitcoin and the use of technologies that are worth billions of dollars.

It's a difficult question, but I would say that this is evolving as we speak. As I said, this morning's mail brought to me a retailer, obviously, who has put together a research project that wants to mine data on children. In terms of identity, the use of our information is what we're now talking about, and the value of it. This is where the billions of dollars come from. It isn't just I, Janet; it's what I mean to someone somewhere else who can use that information to create a product and perhaps undermine a government. This is very sophisticated.

● (1610)

Mrs. Patricia Davidson: I found it very interesting when you were speaking earlier about the app tracking kids' activities, if I understood you correctly. Who okays this? Do the parents have to give permission, or is it school boards? Who participates in this?

Ms. Janet Sherbanowski: In this particular one, and I get these new apps on an ongoing basis, it would be the school, because it's not something that would really raise red flags, “Oh, look, they're going to track how many jumping jacks,” unless you were coming to a committee like this, right?

I will send the link to the committee, because I think it's a very interesting part of what we're discussing. What it's doing is it's looking at jumping as an activity and how many times your child is participating in jumping exercises. It enables school boards to perhaps put together a curriculum based on this, with the child's name, the child's age, and the child's physical activity. We are not going to give that information willingly to someone to track our kids, but through a side road, or a side area, these organizations will be able to track this.

As I said, my concern, in looking at it from a very...I received it literally an hour before I came here. I went in and looked at it, and it's a very neat little program, but I don't necessarily want this information on a little child being used 20 years from now.

Mrs. Patricia Davidson: No, and I guess that begs—

The Chair: Madam Davidson—

Mrs. Patricia Davidson: I have just one quick one.

[*Translation*]

The Chair: Please be quick, Ms. Davidson.

[*English*]

Mrs. Patricia Davidson: It just begs the question: how many people ever know whether or not there has been an identity theft?

Ms. Janet Sherbanowski: I don't think very many of them know at all. This is one of my big difficulties. These are not being reported.

Certainly, the resources are not being given to our police forces to do this. If there is an information area—and I work with the Toronto Police Service financial crimes unit—it's viewed as almost a victimless crime. It's not something that would raise the same types of concerns as an assault, a murder, a robbery, or a theft on the street.

In the crime stats that are being reported, we see everywhere that crime has gone down. One of the big reasons that crime has gone down is that it's not cash that's being carried; it's credit cards or debit cards. This indication that crime has gone down is a misnomer. Crime has not gone down. It's just under-reported.

Mrs. Patricia Davidson: Thank you.

Thanks, Mr. Chair.

The Chair: Thank you very much.

Now I'll give the floor to Mr. Simms for seven minutes as well.

Mr. Scott Simms (Bonavista—Gander—Grand Falls—Windsor, Lib.): Thank you to our guests.

I had a different line of questioning, but as I was listening to Ms. Davidson, what was interesting, and what I find interesting—and I guess my first question is for Ms. Sherbanowski—is that the under-reporting of that type of crime is one thing, but when you're dealing with an area like the one I represent, where there is a high degree of seniors, there is that reluctance to report.

How do you go about doing this? You said that you've worked with New Horizons groups, Ms. Sherbanowski. How do you go about engaging seniors by saying that this is what's happening and here's how to recognize it, and they need to come forward?

● (1615)

Ms. Janet Sherbanowski: New Horizons for Seniors is a federal program from which we receive funding, $25,000, to educate seniors on fraud. We receive a number of invitations, which we are now unable to fulfill, from seniors groups, hospitals, nursing homes, and the City of Toronto's seniors' forum to go out and provide educational material. There is something called “The Little Black Book of Scams” that was produced by the Competition Bureau, which we widely distributed. Unfortunately, it became something that is now available only online. It's a very comprehensive book that can be used for seniors. I would advise you to get some copies of it. I was able to get 200 to give out to various groups, and then I started photocopying. It's a very good resource.

Seniors have a different type of.... You're right: they don't want to report. One of the biggest scams is the romance scam. That encompasses both the fraud side of it and embarrassment for them in regard to getting money from them.

Also, there is the identity theft part of it, because quite often the person who is being proposed as a romantic companion is someone whose identity has been stolen. You have somebody in Indiana, for instance, who is saying that they are a lieutenant in the Marines from the United States. A board member of mine was actually a victim of this. The person ended up asking for $8,000 to come to Canada. By the time this had happened, not only had my friend participated in the scam and shared photographs and information about her own life, including financial details and all of that, but her information could then be used to scam somebody else with her photographs, and that person would be another nice romantic target. It really is perpetuating.

You're right when you say that seniors don't want to report this. When we go to talk to them, I'm of an age that they're certainly able to identify with, so the face-to-face communication is very good for them.

Mr. Scott Simms: Before I move on, what was the name of your resource?

Ms. Janet Sherbanowski: It's called “The Little Black Book of Scams”. It's produced by the federal Competition Bureau.

Mr. Scott Simms: I would like to get copies of that myself.

My next question is for you, Mr. Popa. I hope I've pronounced your name correctly. I'm sorry if I did not.

Sir, you mentioned successes in Europe. Were you talking specifically about cyberfraud, cybercrime, or a combination of the two? Could you outline some of these successes that are practised in Europe? I mean successes in the sense of what we're not doing.

Mr. Claudiu Popa: Sure, thank you for the question.

What we find is that Europol, for example, is an organization that is obviously a law enforcement body, but it's one that is very, very connected with their equivalent in Asia. They have touch points in Canada as well. One of the things they do differently is they publicize a lot of their successes. One of the latest ones has been within the airline industry where there was a tremendous amount of fraud based on identity theft. Those identities were used by people to just fly around the world for millions of dollars' worth of value, but more importantly, with the intrinsic risk of effectively flying these unknown individuals with unknown intentions around the world. That particular success was widely publicized recently, and they said that they are focused just as much on every other industry that is thusly suffering. The reason I mention this one is obviously that it has a particular touch point with our topic of interest.

One of the things they're doing is obviously communicating things. One of the things they're also doing very well is collaborating and exchanging information, so not just saying that they are equally concerned about specific types of crime, but they're actually exchanging behavioural information and transactional data for suspected parties. They do so across a number of layers. For example, we're obviously particularly concerned with corporate identity fraud. Corporate identity fraud is, in many cases, what begins this chain of abuse of trust that leads to personal identity fraud. A lot of this corporate identity fraud, of course, is a concern to corporations. They have an education program that ensures that organizations understand what the impacts are to their reputations, their finances, etc., so they get a lot of support from organizations in Europe in particular.

● (1620)

Mr. Scott Simms: Sorry, I don't mean to interrupt you, but I have one question left.

I find that interesting, because I was in eastern Europe some time ago, and there are several countries now practising open data practices on a large scale, countries like Estonia and Latvia. That trend seems to be spreading through the Nordic countries and further. I guess with the European Union they're going to do much more, so I'm a little surprised with the open data policy, yet they still have best practices for cutting down on cyberfraud and cybercrime.

Mr. Claudiu Popa: They do.

Sorry, was that your question?

Mr. Scott Simms: That's it, yes.

Mr. Claudiu Popa: What I do is I differentiate between open data strategies and proper open data practices. What we're seeing is that some countries are supporting open data activities, but those open data strategies are not necessarily effective. For example, you might have specific countries that are publishing datasets that they simply have no need for. They conduct inventories of the data that they're holding and they're saying they don't really need this data, but before destroying it, they'll just publish it as open data and look really good doing it. That's not necessarily helpful or effective. In many European countries they're actually saying that this is anonymized transactional data that is in fact leading to added intelligence, not just for the creation of apps that we can sell for 99¢ for someone to make money off of, but for law enforcement to say that there's a tangible trend and there's a rate at which people in specific vulnerable sectors are clicking on different things. This was shared by organizations, by associations, by advertising councils and bodies, and that is useful. So I encourage the definition of open data in general versus effective open data sharing.

The Chair: Thank you. The time is up, Mr. Simms.

Now I give the floor to Ms. O'Neill Gordon for seven minutes.

Mrs. Tilly O'Neill Gordon (Miramichi, CPC): I want to thank the presenters. They certainly have shared a lot of worthwhile information with us, and information that gives us food for thought as we go forth in our study.

Following in my colleague's steps, and this question is for Ms. Sherbanowski, is there a basic short list that can be circulated to my constituents to help them protect their identity? Would that be helpful?

Ms. Janet Sherbanowski: Thank you for the question.

There is a short list, and the easy answer is that sure, we can say to do this, this and this. The long answer is that when electricity was first put in, anything electric could be plugged in and there were many house fires. Then we developed grounding and all these things. Everybody's little things that come in from abroad must have CSA approval. I'm sure we've all seen that label. The Canadian Standards Association also does ISO standards and various standards on many things, including information and the standards we should be setting for information.

I think this is what it's going to take. If we truly have an interest in protecting our society, then we as people who are perhaps studying this in greater detail, as electricians studied electricity to protect people, are going to have to develop a risk assessment for things coming through our country and through our firewalls into our homes and bedrooms and wallets.

Privacy by design is something that I think all the privacy commissioners in Canada have looked at. Designing protections into what we allow our corporations to do is going to have to be part of what we as a society do. I know this is something banks and insurance companies and health companies and everybody looks at, but they say that this is going to cost them a lot of money; this is going to be this, that, and the other.

That is going to be a cost of our doing business in the 21st century. I think it's a worthwhile cost.

● (1625)

Mrs. Tilly O'Neill Gordon: Yes, it's a cost that we need to experience in order to make things better for us.

You also mentioned change your PIN day. Is that being successful right across Canada? Are many people taking part in it?

Ms. Janet Sherbanowski: It's something that is being picked up.

I have a proclamation done on March 20. It happens to be my birthday—it also happens to be the first day of spring, in many cases—so it's easy for me to remember. It's much like what we do with the fire alarms and changing the smoke detector. It's something we can remember as a touch point. It's a little bit kitschy, but it's catching on. The other crime prevention groups across Canada have been picking it up, across Ontario. It's something that again I will be presenting through the Competition Bureau.

We send out a press release. At CPAT we invite a seniors group every year and do a luncheon for 50 to 100 people. We invite the Insurance Bureau of Canada and the Bank of Canada to come, and they do a thing about money and fraud. We talk about fraud and send out releases to various seniors groups.

As I said, everybody uses something very memorable, so that you don't have to have too many PINs, but the adding on of the year at the end or at the beginning just makes it a little more unlikely that somebody looking over your shoulder is going to be able to guess it easily. It's just a reminder that we need to be protecting our identity.

Mrs. Tilly O'Neill Gordon: Yes, and it is something that will catch on, like smoke detectors today. Now, that is a common thing, so in years to come this too will be.

Ms. Janet Sherbanowski: I hope so.

Mrs. Tilly O'Neill Gordon: When I listened to you both present today, I thought of at least two constituents who have had the misfortune of losing all their identity by being conned into giving it out, thinking that they were receiving help and were getting benefits on their computer, which they couldn't use. There were troubles there. They felt they were gaining everything. Especially when they're being told that they're getting something back in turn for giving this information, they're very quick to give out the information, regardless of how many times their families and their neighbours and their friends tell them not to. It's just something they walk into.

I'm wondering what new ideas our government can propose to get at this, such as maybe training or courses for seniors. I like the idea you presented of training with New Horizons for Seniors. Even more, with our youth today, there are going to be many incidents in which people are going to get hit with this.

What we can do? Are there any particular aspects of the issue that you would recommend we could help as our study goes on? It certainly is a worthwhile study and one that we're all tuned in to in trying to make things better for everybody.

Ms. Janet Sherbanowski: Is the question for Janet?

Mrs. Tilly O'Neill Gordon: For both of you, if I have time.

Ms. Janet Sherbanowski: All right.

If I may start, we founded the Social Media Working Group with the Toronto Police Service. It involves the Insurance Bureau of Canada, all the banks, Bell Canada, a lot of groups, and the school boards. Twice a year we do a fraud conference in Toronto. It's televised on Rogers and it's also available on the Toronto Police Service's website.

The first one we did looked at working with the media, having all the media come in and listen to all the experts. It was started just last year, so it's fairly new for Toronto. We work with PhoneBusters and CARP. It has grown. Even the Public Guardian and Trustee is now part of this. Health fraud and identity theft go on. It's an education process.

● (1630)

The Chair: Thank you, Madam Gordon.

[*Translation*]

I am told that the time that we had with our witnesses has run out.

Many thanks to Ms. Sherbanowski for her time today. My thanks also go to Mr. Popa, who was in Florida and I hope he enjoys the rest of his vacation. Our witnesses' expertise on the issue will definitely help us to move to the next part of our study.

On that note, I suspend the meeting for a few minutes.

[*English*]

Mr. Claudiu Popa: That's no problem. Thank you for having us.

The Chair: Thank you.

I will suspend for a couple of minutes to go in camera for committee business.

[*Proceedings continue in camera*]