HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 019 • 2nd SESSION • 41st PARLIAMENT

EVIDENCE

Tuesday, April 29, 2014

Chair

Mr. Pat Martin

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, April 29, 2014

● (1100)

[*English*]

The Chair (Mr. Pat Martin (Winnipeg Centre, NDP)): Good morning, ladies and gentlemen.

Welcome to meeting 19 of the Standing Committee on Access to Information, Privacy and Ethics. We will continue our study of the growing problem of identity theft and its economic impact.

We are pleased to welcome José Manuel Fernandez, an assistant professor in the department of computer and software engineering at École Polytechnique de Montréal. Welcome, Professor Fernandez.

We also have Susan Sproule, an assistant professor of finance, operations and information systems at Brock University. Welcome, Ms. Sproule.

By video conference, we welcome Mr. Benoît Dupont, the director of the International Centre for Comparative Criminology, from Montreal. Welcome.

From Whitehorse, Yukon, via video conference—which is quite a commitment to make; it must be very early there—we welcome someone who's no stranger to this committee: Philippa Lawson, a barrister and solicitor and an associate of the Canadian Internet Policy and Public Interest Clinic at the University of Ottawa. Thank you very much for being with us here today, Ms. Lawson.

We begin with opening remarks. I think we'll start with those who are present with us in attendance.

Professor Fernandez, we invite you to make opening remarks of five or ten minutes. The floor is yours, sir.

[*Translation*]

Mr. José Manuel Fernandez (Assistant Professor, Department of Computer and Software Engineering, École Polytechnique de Montréal, As an Individual): Thank you, Mr. Chairman.

Good morning, ladies and gentlemen.

First of all, let me congratulate you all for making the decision to address the important problem of identity theft in Canada. Let me also thank you for inviting me here today. This provides me with the opportunity to bring this problem into perspective as it relates to other problems concerning Canadians.

[*English*]

Let me congratulate you also on your uncanny serendipity and your impeccable sense of timing, especially considering the events related to the Heartbleed vulnerability of the last few weeks. When I got the invitation to testify before this committee a few days after the events, I thought that these parliamentarians were really quick to react or they knew something about the bug that I didn't know.

As you know, the Heartbleed bug affected the web servers of the Canada Revenue Agency, and despite the diligent efforts of the IT professionals of government, which should be commended, this led to the unauthorized disclosure of at least 900 social insurance numbers of Canadian taxpayers.

This underlines the real risk about the way we are using IT infrastructure and what it represents in terms of risks for identity theft. Such events, and the media interest that they generate, are great opportunities for experts like me to bring the message. However, sometimes the media attention and the way the story develops can backfire, and it brings attention to the wrong things.

Heartbleed is not about the computer whiz kid who was arrested by the RCMP in London two weeks ago and is being accused of hacking the CRA servers. It's about a bug that affected two-thirds of the web servers on the planet. By the time this kid got to the CRA servers, thousands of other hackers had hacked tens of thousands, if not hundreds of thousands, of servers worldwide. Heartbleed is really about the pitiful state of our information infrastructure and how we have let it become that way.

What has that got to do with identity theft, you will ask? The social insurance numbers that were leaked could lead, with enough other personal information, to helping cybercriminals conduct identity theft, in activities like fraudulent banking transactions, a destruction of credit history, and unauthorized access to computer email accounts and social network accounts.

Other witnesses to this committee will certainly testify to various nefarious effects of identity theft to Canadians and to Canadian businesses. What I'm here to tell you today is that, maybe to your surprise, identity theft is not the problem. Identity theft is one problem among many, and is probably one of the least important ones at that. It's only the visible tip of the iceberg. It's a problem that your electors are probably calling your riding offices about because that's what they feel in their skin. However, it's not really the one that is looming highest regarding their welfare.

What is the problem, then, or rather what are those bigger problems that we should be worrying about as well? That's easy: cybercrime, cyber-espionage, cybersabotage, and their impending doom.

My colleagues Benoît Dupont and Susan Sproule will certainly talk to you about figures and the size of the problem of cybercrime, and identity theft in particular. But to give you a few examples at my level as an engineer, credible experts have estimated the cost of cybercrime worldwide at hundreds of billions of dollars a year. In Canada, Symantec estimated the cost of cybercrime in Canada, in 2013, at $3 billion alone. That's 60% of the budget of the City of Montreal, where I live, and it certainly could use that money.

Cybercriminals use infected computers in corporations, government offices, and in homes of unsuspecting consumers, to turn a profit by a variety of means. This can include Internet banking fraud, which is the most common, but also Internet publicity fraud, extortion, and also traditional forms of fraud and con artistry.

Cybercrime is alive and well. It's a growth industry, with international ramifications. It involves a complex network of criminal groups that work together. To give you an idea of the size of the problem from a technical point of view, some surveys published in the European Union are reporting that 30% to 35% of users are reporting that their machines were infected in the last year. We thought that this was *un petit peu d'exagération européenne*. We thought that these Europeans had a sense of exaggeration and colourful language.

● (1105)

To our surprise, when we did research at Polytechnique in 2012 where we conducted a clinical trial with 50 subjects and we monitored their computer activity for four months, we discovered that 5% of them got infected by dangerous malware and 20% of them got infected by some kind of harmful software, and that's despite the fact that they had an anti-virus installed.

Further analysis showed that if none of them had any anti-virus installed, 38% of them would have been infected. That's two out of five Canadians whose computers are potentially infected.

So maybe the Europeans were not exaggerating so much after all. But beyond its sheer economic impact, the problem with cybercrime is that it generates phenomenal profits. These cybercriminals have been investing that money in R and D, in research and development. They've been developing hacking tools and techniques that baffle us, the computer security experts in the computer security industry. They have more money than us. They have certainly more research budgets than I do at Polytechnique and it's probable that they have overall been investing more R and D in developing the tools than all of the computer security industry. So we're losing the war. We are in an arms race and from a technical point of view we're losing and we know that. We don't say it very often very publicly, but it is true.

Why should we care about cybercrime so much? Relatively few Canadians are affected. It's in the few per cent in terms of financial loss and most of the time the banks do pay. The problem is that the banks are starting not to pay. That's good for me because I get to go to court and testify and tell the judges that sometimes, yes, the banks should pay and that's good for me, but it's not good for Canadians because the tendency is about to revert. I've had more and more of those cases happening.

Also, cybercrime is not cancer. It's not unemployment. It's not global warming. It's not car accidents, so why should we care about it? Nobody dies of it.

The problem is that this technological advantage that the cybercriminals have been developing has been used for other things now. The first and most historically significant example politically was that of child pornographers. Child pornographers started using Internet technology and hacking tools in the 1990s and that prompted the development of specialized teams in law enforcement. We helped at Polytechnique by creating a program to train those policemen.

That's not even the biggest problem. What has become clear in the last few years is that the bigger threats lie in cyber-espionage and cybersabotage. We're just starting to find out right now how much foreign intelligence agencies and foreign economic interests have been rifling through our computers here, government computers, Canadian businesses, and Canadian citizens, for over a decade.

We in Canada were not the victim of the denial-of-service attacks that essentially obliterated from the Internet planet countries like Estonia and Georgia in 2007 and 2008, or the production of weapons-grade uranium was not halted by a computer virus in 2010 like Iran's was and that's a good thing because we don't make weapons-grade uranium in this country. Also, our oil companies, because we do have those, were not forced to replace 30,000 desktops overnight like Saudi Arabia's Aramco had to do in 2012 because of a patriotic vengeful hacking group from Iran.

We have not been the victim of these very huge metadata attacks, but there's no shortage of significant incidents and some of those are becoming public. It is possible and it has been said that the laptop of the CEO of Nortel was compromised by Chinese hackers since 2001. I will ask you now who is the second-biggest provider of networking equipment in the world, having replaced Nortel?

In a recent incident, the source code, which is the secret sauce that runs some of the components of a critical infrastructure, including the energy infrastructure.... The source code for that was stolen through a computer hacking attack at a Calgary-based company called Telvent, which is a provider of a lot of our critical infrastructure.

● (1110)

What keeps me up at night is not identity theft; it's this stuff. Imagine the ice storm of 1998 in southern Quebec and Ontario; I was there. Three million Canadians were without electricity for a week, and several hundred thousand of those were without electricity for up to a month in the middle of the winter. Imagine that this was not a freak of nature, that somebody did this from somewhere on a laptop with a click, and could do it again. This is real. It could happen. It's worse than identity theft. It's theft from the economy. It's national security theft. It's click, no economy; click, no national security; click, no governability. Imagine the loss of confidence of Canadians in our government.

You will say this is not the mandate of this committee, but I would say that it is definitely within the mandate of government. You certainly have colleagues, members of Parliament in other committees, such as the public safety and national security committee and the industry, science and technology committee, and I would encourage you to talk with them and work with them. The reason is very simple. Deep inside, at the end of the day, this is the same problem. The root causes of the problem of identity theft, cyber-espionage, cybersabotage, you name it, are all the same. It's the way we've been running our IT infrastructure and the way we've been looking the other way and enjoying all the gadgets.

What are these causes that we can try to start addressing?

The first one is that there have always been crooks and there always will be. Where there's a buck, there's always a thief, and the Internet is no exception. They've just moved to the Internet.

The second one is the way we've used computer and Internet technology was never meant or created for the purposes that we are using it. A case in point is the World Wide Web. The World Wide Web was invented by researchers in Switzerland to have an interactive way of sharing research data, and 30 years later it's running the worldwide economy. It wasn't meant for that. It wasn't built with the appropriate security mechanisms and accountability.

The technological solutions exist. They've been developed. They're all there. We know them. In engineering schools, we teach them, but the forces and incentives to put them to work never seem to be there. It's always the same thing. Apathy, ignorance, and vested interests that are not in the best interest of the public are preventing these things from being deployed, enhancing our lives.

The third one is the fact that the IT industry in historical terms is still relatively young and immature. Thirty years ago computers were relatively isolated. A few crazy people like me had personal computers. The fact that this was a deregulated, completely improvised industry was okay. This is akin to what the car industry was like at the turn of the 20th century. There weren't that many cars on the roads. They were quite noisy, but they weren't that fast.

But the post-war era came, the crazy twenties, and the cars became bigger and faster, and there were starting to be some car accidents. Then after World War II and the big boom, the baby boomers—this is where they came from—there was also the car boom. The cars became fast, and superhighways were built in Canada and the United States. Then the problem blew out of proportion. We're talking about tens of thousands of deaths a year. Something had to be done, and it was done.

Engineering standards were applied to the manufacturing and inspection of autos and parts. Professional engineers were the only ones allowed to design and certify critical components. Governments worldwide wrote and imposed mandatory safety standards on the industry. Highway codes were enacted, and drivers' licences and driver training became mandatory. Even the lawyers helped. They started suing people and industry for carelessness and neglect. Even the insurance companies chipped in. They imposed standards of their own. That's how seat belts became mandatory and safe. Eventually even the Criminal Code was amended. Impaired driving became a crime. You could go to jail. That wasn't the case before. Finally, even technology and law enforcement married up and came up with some law enforcement technologies, such as the breathalyzer and radar gun.

● (1115)

This is where we are right now in the computer industry by comparison. We are somewhere in the early 1950s. The "information superhighway" as it was called by Al Gore, the Internet, has been built and it is travelled by millions, by billions, every day. The cars are big now—the computers—and people use them for all kinds of things. They look fancy, and we all want the fastest and the coolest model. Our economy and our way of life depend on them. In fact, we are addicted to the freedom these computers provide us in the same way we are addicted to cars. The difference is that "computer accidents" don't kill people...yet. Just wait, it will happen.

[*Translation*]

In conclusion, while addressing the root causes of the problem, we'll need to involve many different sectors of society including professional associations, educators, industry, civil servants and law enforcement. It is chiefly with you, as lawmakers and members of Parliament and government, that the responsibility to lead us away from this mess lies.

But you are not alone. We, who have created Pandora's box, saw others open it despite our warnings and would like nothing more than to help close it.

Thank you very much for your attention.

● (1120)

[*English*]

The Chair: Thank you very much, Professor Fernandez, for those very sobering opening remarks.

We'll proceed right away to Susan Sproule from Brock University.

Madame Sproule, you have the floor.

Dr. Susan Sproule (Assistant Professor, Finance, Operations and Information Systems, Brock University, As an Individual): Good morning.

My involvement with the subject of identity theft started in 2005 with a research project that involved four universities and subject matter experts from the financial sector. My group was assigned the task of defining and measuring identity theft. On the measuring side we did a comprehensive survey of Canadian consumers in 2008, but that data is really too old to have much value now, so I'm going to concentrate on the definition problem and then discuss some of the difficulties in measuring identity theft. I hope that can help provide some guidance for your study.

To come up with definitions, we started by trying to organize some of the activities that came up frequently when we were discussing identity theft. I had a diagram. I don't know if you've been given copies of it, but basically at the beginning we had a number of activities that described different ways that identity information can be collected. In the middle we had a number of activities that were involved in the development of a false identity, things like counterfeiting documents and document breeding. Then at the bottom we had crimes that are enabled by a false identity.

We were just looking for working definitions that our various research groups could agree on. In a series of workshops, we decided that identity theft should include all the illegal ways of collecting information and all the activities in that development of a false identity. These are preliminary activities to a fraud.

We said that ID fraud should include all the crimes where the use of a false identity was integral to the crime. In other words, you might want to use a false identity if you're smuggling drugs, because that would be useful if you get caught, but you can still smuggle drugs without using a false identity, so we said that's not identity fraud.

I won't go through our formal definitions, but we were quite pleasantly surprised that our definitions ended up to be very similar to those that the federal government's Department of Justice came up with as they prepared the ID theft legislation introduced in 2009.

A key point from all of this is that identity theft and identity fraud are two different problems. Identity theft is a problem of personal and agency guardianship, that is, keeping personal information secure. Identity fraud is a problem of authentication, or being able to determine that the person who is presenting identification is really who they say they are.

Why is this distinction important? You can have one without the other, and vice versa. The thief and the fraudster are usually different people. In general, identity thieves steal identity information and sell it to identity fraudsters. We notice that cases of identity theft—data breaches, etc.—are rarely linked to cases of identity fraud, because there's this middle area that the information goes through.

Primarily, it helps us to focus on the interest and responsibilities of the stakeholders. So, as an identity owner, I can help prevent some identity theft. I can keep personal items that contain identity information secure and not give out personal information unnecessarily. I really have no ability at all to prevent identity fraud. Once my information has been compromised, the only thing I can do is help detect it and report it as soon as possible.

But as an active participant in life today, I really have no choice but to give personal information to all kinds of organizations. These organizations have roles in preventing both identity theft and identity fraud. They can prevent identity theft by keeping any of my information they possess secure. They can prevent identity fraud by ensuring they have proper authentication processes in place whenever identification is issued or is checked.

Organizations are also responsible for detecting both identity theft, when information has been compromised, and identity fraud when these processes have failed and fraud has occurred.

● (1125)

Even within an organization, if you try to interview an organization about identity theft and fraud, the responsibilities for those two problems lie in different areas of the organization. Who is responsible for the guardianship problem? It's generally the security department when we're talking about physical security, and it's the IT department when we're talking about systems security. Who is responsible for the authentication problem? That's anyone who's involved in designing, or managing, or even conducting all the business processes around all kinds of transactions.

On the topic of measuring identity theft and fraud, there are lots of challenges. The very first comes back to this whole problem of defining. A 2006 Ipsos Reid survey found that 29% of Canadians agreed with this statement: “I hear a lot about identity theft, but I don't know what it means.” So if you want to do a survey to find out the extent of identity fraud, you can't just ask respondents if they have been a victim. Many surveys do this, but you really can't interpret anything valuable from these results. In our survey, we gave very specific examples of the various types of identity fraud that we were interested in.

Besides doing surveys, you can look at reports of identity theft to such organizations as the Canadian Anti-Fraud Centre, but the second problem is a general lack of reporting. Credit card fraud and debit card fraud are investigated and handled internally by the credit card companies and the banks. Only a small proportion of those cases are ever referred to police. A Statistics Canada survey on fraud in retail businesses showed that between 40% and 50% of cases were never reported to police. Less than 40% of individual victims ever report to police.

Why does this happen? In general, businesses are afraid of negative publicity. People are embarrassed that they fell for a scam or that they didn't protect their information. I think both often believe that police can't do anything, and they're right, in many cases.

In terms of costs—I gather it's part of your mandate to look at that—the costs of identity theft are many, and they are borne by individuals, by organizations, and by society. Individual victims are not held responsible for financial losses once it's established that a fraud has occurred, but they often have significant costs getting to that point in terms of time and a lot of frustration and anxiety.

Organizations bear most of the monetary losses associated with ID theft and fraud. There are two problems associated with that. First, organizations are very reluctant to tell anybody what these costs are. Secondly, the costs alone don't provide strong incentives to prevent identity theft and fraud.

When an organization has losses associated with identity fraud, those losses are simply passed on to consumers in the form of higher prices, fees, or rates. As well, in Canada the lack of breach notification requirements means that Canadian organizations do not necessarily even suffer from reputational damage. I understand that the proposed digital privacy act will be taking some steps in that direction, and that's a good thing.

There are also general costs to society in the form of a chilling effect. Different studies, including ours, show that between 20% and 40% of consumers say they have adjusted their online behaviours because of a fear of identity theft. This means that Canadian businesses are not benefiting from all of the advantages that electronic commerce should be bringing.

There are two things I would like to see addressed in your study.

First, I would like to see greater responsiveness to consumers by the credit reporting agencies. As I've said, the one thing that individuals can do is help detect frauds, but if we want them to take these steps, they need greater access to and greater control over their credit files. Credit reporting agencies have to provide a free copy of your credit report each year, but they make this as difficult as possible. To get a free copy, you have to fill out a form, copy a multitude of documents, send it all off in the mail, and wait a couple of week for them to mail you back a report. They provide online service. Online service is more secure, and it has to be less expensive to provide, but they'll charge you $24 for that.

● (1130)

As well, both of the credit reporting agencies offer ID theft protection products for $15 to $17 a month. By offering these products, they are profiting from the problem, which provides little incentive for them to reduce or eliminate the threats.

Finally, it's very difficult to manage something if you aren't measuring it. We need regular, periodic data collection in order to identify trends and to design effective educational initiatives and effective policy. Since there isn't one single measure for identity theft and fraud, we believe the real need is for an identity theft and fraud index that would work like a consumer price index or purchasing activity index. This index would bring in information from regular surveys of consumers, surveys of businesses, as well as reports from law enforcement, from credit reporting agencies, from privacy commissioners, victim services, and any other groups.

Thank you for your attention, I hope that's helpful.

The Chair: Thank you very much, Professor Sproule.

I'm sure committee members will have some questions for you when the time comes. Thank you.

Next then we'll go—by video conference—to Benoît Dupont, director of the International Centre for Comparative Criminology.

Monsieur Dupont, go ahead.

Dr. Benoît Dupont (Director, International Centre for Comparative Criminology): Good morning and thank you, Mr. Chairman and honourable members of the committee, for inviting me to participate in these proceedings.

As you said, I am the director of the International Centre for Comparative Criminology and I also hold the Canada research chair in security, identity and technology at the Université de Montréal, where I've studied the issue of identity theft for the past seven years or so.

In the 10 minutes that I have at my disposal, I would like to briefly address some issues about this very complex form of offending and the harms it causes to Canadians. But before I go any further I would like to maybe state that the term identity theft is perhaps a bit misleading because it implies that the victim loses access to their identity like when you lose access to a car or your cellphone when it's stolen, while in fact, the victim is more deprived of certain benefits associated with full control over their personal information such as a high credit rating or the ability to secure a bank loan. I think it would be more useful to use the terminology of identity manipulation or identity-related crime, but I guess it's way too late now to change the terminology. But I think it's an important matter as well.

So I think your task here is very important and by reading the transcripts of the sessions that were already held, one can be sure that we will learn lots in the process and in the report that you will produce. Therefore my comments today will be slightly different, as I would like to address briefly a list of four things I believe we don't know about when we talk about identity theft and how addressing this knowledge gap would help us design more effective preventative strategies and also more effective regulatory tools. These are the, if you like, known unknowns to paraphrase a very famous American politician.

The first unknown that my colleague Susan Sproule talked about is the current size of the problem in terms of the actual number of victims and the evolution of this trend. I read the transcript of the RCMP testimony and the person representing the RCMP stated that 24,000 victims contacted the organization in 2013 following instances of identity theft. This is probably a tiny fraction of the overall pool of victims because most of them, as my colleague Sproule said, never lodge a formal complaint with their police service, some of them because they don't believe the crime is important enough or will attract any interest, others because they're discouraged by their local police service, which is not equipped to deal with this type of crime especially if the amounts involved are below a certain threshold.

To provide you with a hint of a more realistic assessment, in 2009 a victimization survey conducted by Statistics Canada across a very large sample of the population evaluated that more than 870,000 Canadians had been victims of Internet bank fraud over the past year, which does not include other forms of fraud associated with identity theft. These are huge numbers but in technology terms, five years is an awfully long time and we don't have any reliable statistics on an annual basis to assess the severity of the ID theft problem and the effectiveness of current strategies to address it.

The second thing we don't know very well is that we don't have a clear breakdown of the types of ID theft by sources of stolen credentials or fraud stratagems used by offenders to exploit them. I conducted a survey very similar to the one conducted by Susan Sproule in 2007 in Quebec and this survey showed that online scams such as phishing emails only amounted to 6% of the stolen personal information, while card skimming or the theft of personal information by organizational insiders amounted to 55% of cases. Since then, I have not seen any updated information relevant to the Canadian situation, although again the technology has changed a lot during the past seven years and probably a larger proportion of Canadians conduct their business and financial transactions online.

Thirdly, we don't know a lot about identity thieves and whether they're a traditional category of offenders who have migrated to this new profitable market or a brand new breed of offenders with very different sets of criminal skills and modes of social organization.

● (1135)

We do know that a small number of them are very successful and are able to obtain, through elaborate cyberattacks, millions of stolen records that they resell in underground markets, such as was the case with Winners or the more recent Target hacks where tens of millions, and in certain of cases hundreds of millions, of credit card numbers were stolen from large retail companies. We still know very little about these markets, how they operate, and how much of the stolen information belongs to Canadian consumers.

We don't really know which organizations are more effective, which ones are more exposed, and which ones do a good job at preventing identity theft. We know that banks invest a lot of their money in anti-fraud technologies. They are very advanced in their capacity to identify and block attempts at ID theft. But we don't know which one of the five or six big banks perform the best, and also the worst, and what types of retail or service businesses are leaking disproportionate amounts of personal information to offenders. All organizations are not equal when faced with the problem of identity theft.

You may ask, why would this knowledge be useful? This would help us design and implement more effective prevention strategies that would target and reinforce the weakest points in the payment ecosystem first.

Second, it would also better inform us about the need to create new regulatory tools in the area that would compel companies to protect consumers' personal information and notify them when needed not only from a privacy perspective but also from a security perspective. It would also help us make sure these regulatory tools are reasonable and do not unduly burden businesses.

Finally, I think it would help us and it would especially help law enforcement agencies focus their limited resources on the most dangerous and prolific offender networks.

However, I wouldn't like to end on a pessimistic note. There are causes to be optimistic. We shouldn't be desperate about the problem of identity theft. For example, the introduction of the chip and PIN technology in Canada on our credit and debit cards over the past few years as well as advances in anti-fraud technologies deployed by the banking sector have produced tremendous reductions in related identity theft and fraud, illustrating that sometimes organizational changes can produce systemic outcomes at the national level.

For example, if you look at Interac statistics.... I took these statistics off the Internet and put them together in a slightly different way than Interac. Between 2004 and 2012 the global amounts of dollar losses attributed to fraud by Interac—if we accept that this data is accurate—has decreased by 36%. During this same period, the amount of transactions conducted by debit card had increased by 53%. So fraud is decreasing and the number of transactions are increasing.

For credit cards, we have a similar trend where the global dollar losses between 1999 and 2012 increased by 94%, and that's a lot. But this is only about half of the 212% increase in the total amount of credit card transactions over the same period.

So the average loss per dollar transacted through Interac is about 2¢ and the average loss per dollar transacted through credit cards is about one-sixth of a cent. This ratio has not really changed over the past 10 years, which is quite reassuring, because the problem of identity theft is not as dire as sometimes some private companies make it up to be.

The problem we have with the chip and PIN is that, of course, our neighbours to the south have been slower to adopt this technology. This leaves many opportunities for offenders to exploit the data captured from the back of the credit and debit cards on the magnetic stripes.

● (1140)

Thank you for your attention. This concludes my comments. Of course, I welcome your questions. Thank you.

The Chair: Thank you very much, Mr. Dupont. That's very useful and very helpful.

Finally, then—and thank you for your patience—we have Philippa Lawson, University of Ottawa, Canadian Internet Policy and Public Interest Clinic. Thank you very much for being with us here today, Ms. Lawson. It's your turn.

Ms. Philippa Lawson (Barrister and Solicitor, Associate, Canadian Internet Policy and Public Interest Clinic, University of Ottawa, As an Individual): Thank you, and good morning, Mr. Chair and committee members.

Thank you for inviting me to address you today on the issue of identity theft. I have been studying and working on this issue from the consumer and victim perspective for over 10 years, first with the Public Interest Advocacy Centre, then with the Canadian Internet Policy and Public Interest Clinic or CIPPIC, the International Centre for Criminal Law Reform and Criminal Justice Policy; and most recently for the Canadian Identity Theft Support Centre.

l've provided a list of publications with my speaking notes today, and I hope that will be distributed to you. These publications include analyses of the range and types of identity-related crime, an international inventory of best practices for victim remediation in both public and private sectors, a gap analysis of legal rights and remedies for victims of identity crime in Canada compared to the United States, and self-help guides for Canadian victims of identity theft. These are all accessible online.

In my capacity as director of CIPPIC, I made submissions to this very committee when it was studying the issue of identity theft back in May 2007. Looking back on those submissions, they are, for the most part, as relevant now as they were then. There have been some developments in the last few years, notably amending the Criminal Code to make it easier for law enforcement to catch and convict identity thieves, which is an important step but only one of many tools needed to address the problem; and also establishing the Canadian Identity Theft Victim Support Centre, which can now be found online at www.idtheftsupportcentre.org, or via its 1-866 hotline. But much more can and should be done to prevent, detect, prosecute, and mitigate the effects of identity-related crime.

I understand that you are interested in the economic impact of identity theft in Canada and that your focus is on privacy or identity-related crime as opposed to mass market frauds generally, or cybercrime generally. I cannot give you any numbers. For the reasons my colleagues have stated, I doubt that it is possible to come up with a good estimate, given the dearth of data on identity-related crime in Canada. Instead, I'd like to use my time just to make five suggestions for policy and law reform in this area.

First, enact security breach notification laws. Individuals can take all the recommended precautions against identity theft, but they can't control what organizations do with their personal data in the custody of the organization. In this age of databases, strong corporate security safeguards are essential to protect against identity theft. Yet, under pressure to cut costs, many organizations are not taking the measures that they should to protect customer data.

A law requiring that organizations report security breaches to the Privacy Commissioner, as well as to affected individuals, would go a long way toward preventing the kinds of security breaches that feed identity criminals. It would also make potential victims aware of their vulnerability, allowing them to take preventative measures before the damage is done. I applaud the efforts of committee member Ms. Borg in this respect, and I encourage the government to consider the private member's bill she has put forward on this issue.

Bill S-4, the new digital privacy act, is a welcome government initiative as it would also require breach notification, but its proposed standard for reporting breaches to the Privacy Commissioner, as opposed to individuals, is inappropriately high, allowing corporations to avoid accountability for inadequate security measures. I know you'll be looking at this bill when it comes before you, and I hope you will look at this very closely.

● (1145)

Second, make data protection laws enforceable. We live in a world of huge and expanding databases of personal information. These are gold mines for identity criminals as well as for marketers, researchers, and even political parties. The Personal Information Protection and Electronic Documents Act, which I'll refer to as PIPEDA, is supposed to protect consumers from the kinds of practices that lead to identity theft and fraud, but practices that violate PIPEDA continue to be widespread in the marketplace. The problem is that PIPEDA lacks teeth. Corporations need not take it very seriously.

The digital privacy act, Bill S-4, would make it easier for the Privacy Commissioner to name and shame corporate offenders. It would also allow the Privacy Commissioner to take action against those who fail to adhere to compliance agreements. These are significant improvements that would make the bill more effective and would be used to hold non-compliant organizations accountable for the kinds of practices that facilitate identity theft, but more could be done to make the data protection laws effective. I hope you will look at all options when Bill S-4 comes before you.

Third, require that credit freezes be offered to Canadian consumers. The messiest form of identity theft is new-account fraud, that is, where criminals use stolen data to create new accounts or take out loans or mortgages in the name of the victim. It can be months before a victim becomes aware of the problem, during which time multiple accounts have been opened and unpaid bills have been run up in the victim's name. Even after the victim succeeds in closing the accounts and dealing with the debts—this is a nightmare in and of itself—the victim can end up paying higher interest rates for years because of their corrupted credit histories.

This may not happen often, but when it happens, it is at a high cost to the individual. By far the best protection against new-account fraud is a credit freeze. A credit freeze bars the credit bureaus from issuing your credit report—the summary of loans and payments that forms the basis of your credit score. Because few lenders will issue credit without first seeing a credit score, identity thieves can't use stolen data to open up new accounts where the credit report is frozen. Credit freezes are particularly helpful for elderly people or for those who don't need to borrow money.

The credit bureau industry has no interest in offering credit freezes for obvious reasons. Doing so would eat into the industry's core business of providing credit reports. However, despite strong industry resistance in the United States, almost all states in the U. S. now require that credit freezes be offered to consumers at no fee or at a very low fee. The reason is to prevent identity theft. There is no good reason why Canadians are not offered similar protection. This is an area of provincial responsibility, but in my view the federal government should be working with the provinces, through, for example, the Consumer Measures Committee to ensure that consumers across Canada have the tools they need to prevent, detect, and mitigate the effects of identity crime, including the ability to freeze their credit reports upon request.

Fourth, coordinate victim assistance initiatives. The Canadian Identity Theft Support Centre, which I'll refer to as the victims support centre, was established in early 2012 with funding from the federal government to provide victims of identity theft with information and support. It has a very specific mandate, and that's all it is. The victims support centre is taking about 10 calls per day now from victims and others inquiring about identity theft, more when there is publicity about the centre. It offers victims hand-holding through the coping and remediation process, which can be extensive.

● (1150)

I understand that the victims support centre provides data to the Canadian Anti-Fraud Centre, but strangely, the Anti-Fraud Centre does not even acknowledge the existence of the victims support centre. Needless to say, there needs to be some coordination and cooperation between these two government-funded agencies so that each can focus on its mandate rather than trying to compete with the other for funds and public profile.

Finally, I would suggest that Canada develop a national strategy for combatting identity-related crime. The four measures I've advocated are just a few of many that are needed to address the many angles of this problem. Canada needs a national strategy to understand and address the specific problem of identity-related crime, a strategy that should be driven by high-level officials and that should involve all key stakeholders. The RCMP's national strategy, which it issued in 2012, is a good start, but it needs a lot more work to get beyond broad generalities and to include the consumer protection angle.

The first pillar of a national strategy should be to develop mechanisms to gather reliable, reasonably comprehensive data on the incidence, types, and costs of identity crime in Canada. On this, I fully endorse the comments of my colleagues, Drs. Sproule and Dupont, on this critical first step in addressing the problem. We need to know the nature of the problem in order to address it effectively. We simply don't have the data in Canada yet.

Finally, sometimes we can learn from our neighbours to the south, and I would suggest that this is one of those times. In 2006, the U.S. President established a special task force to develop a comprehensive national strategy to combat identity theft. The President's task force was co-chaired by the U.S. Attorney General and the chairman of the Federal Trade Commission. It included high-level executives from all pertinent government agencies. Over the course of a year, they examined the problem from all angles and published a comprehensive strategic plan for combatting identity theft in the United States. The plan, which called for a coordinated national approach to policy and law reform, has been largely implemented. There is a lead agency—the Federal Trade Commission—and consumers and victims in the United States now have many more tools at their disposal to prevent and deal with identity theft than do Canadians.

Mr. Chair, and members of the committee, it's time, in my view, for Canada to seize this issue and develop a similar strategy that involves all stakeholders, including consumer protection agencies and privacy commissioners at both federal and provincial levels.

We can do better.

Thank you.

● (1155)

The Chair: Thank you very much, Ms. Lawson.

Thank you to all of our witnesses for four excellent presentations. We would benefit from more time with all of you, I'm sure. We're lucky to have such leading authorities on the subject all clustered into one day.

We used one clean hour for the presentations. That leaves us one full hour for questions. Without any delay, we'll go to the official opposition, beginning with Charmaine Borg.

Charmaine, go ahead, for seven minutes please.

[*Translation*]

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

I would like to thank all the witnesses for attending our meeting today. I would also like to thank them for their excellent testimony that has added some good points to our discussion.

I am going to ask you my first question. I have many questions and it is difficult to choose the one I am going to ask you first.

You all stated that in Canada there is a lack of data on the problems posed by identity theft, data loss and data breaches. For example, the lack of a mandatory notification system in Canada when data is lost or breached, has contributed to the problem because the privacy commissioner is not made aware of these situations.

Could you comment on that?

I also have a question specifically for you, Mr. Fernandez. Given that you focus on the technology development sector, perhaps you actually deal with this issue. Has it interfered with your ability to design security systems that could resolve problems related to identity theft?

Mr. José Manuel Fernandez: Yes, and the lack of data is a problem not only in terms of the government being able to understand the problem, but also in terms of our capacity to undertake research and development for the purposes of finding security solutions.

As Mr. Dupont stated, not all organizations are the same. Some are using management or technological procedures, and some are more efficient than others. In order to be able to determine which ones are better and should become best practices, we need data that will confirm that the measures in question are appropriate.

Data is necessary for research and development, but it is also necessary for another risk management tool, which is insurance.

[*English*]

The insurance industry has been trying to get into the business of insuring Canadians for IT risk and risks like identify theft. But it's a bit of the chicken and the egg conundrum here because they don't have data so they can't evaluate the risk, they can't price the insurance premiums, and therefore they're not jumping into the business.

There are two ways of addressing the problem. One is laws that would force those who had been breached to release that information such that insurance companies and other industry-wide associations could gather that data to start offering insurance premiums. Second, as we've had in other sectors, when the private sector doesn't know how to make money, one option is for the government to start offering those services until enough data is provided and then they can farm out that insurance sector.

For example in Quebec, automobile insurance is a state-owned business. In many other parts of the country it has been privatized. The reason it was created at the beginning, in the sixties I believe, is that nobody from the private sector wanted to own that risk. So I think this is where the government can show leadership, not only in the law but also trying to jump start the process by offering this risk protection.

[*Translation*]

Ms. Charmaine Borg: Thank you.

Ms. Sproule, Mr. Dupont or Ms. Lawson, do you have any other comments?

● (1200)

[*English*]

Dr. Benoît Dupont: I'll just say a few words. I think in terms of the lack of data there are two issues. There is the data that exists already, which is fragmented, and that we need to find incentives, sometimes negative incentives, for organizations to make this data public and available, and to aggregate it and consolidate it. Then there is the data that we need to collect because no one else has it. The perfect example is the victimization survey. Statistics Canada collects this data every four or five years, and with the trend of technology and the speed of this phenomenon I think we need to collect this data on a much more regular basis.

This is not a very expensive undertaking. Running a Canada-wide survey wouldn't cost a lot of money, but it would need to be conducted by a lead agency. I like this idea of having one lead agency being responsible for this issue and being funded to try to collect and to consolidate the existing data.

Thank you.

Ms. Philippa Lawson: Could I add to that?

The Chair: Certainly, Ms. Lawson.

Ms. Philippa Lawson: On the issue of collecting data, information on financial identity fraud exists. It's in the hands of financial institutions and credit bureaus. So I think the government should be looking at ways to get that data from industry.

The Chair: Thank you, Ms. Lawson.

Dr. Sproule.

Dr. Susan Sproule: Certainly information about data breaches and notification requirements for data breaches are a big part of the information that we need to gather to look at the problem, but it's just one part.

As I said, it's very difficult to establish relationships between the identity thefts, data breaches, and actual fraud. The U.S. government accountability office did a study in the early 2000s that said we can't make any connection between all these data breaches and what's happening as far as fraud is concerned, so it's back to the idea of an index. We need information from a lot of different sources, I think, to be able to put the whole picture together. We need victim surveys. We need surveys of businesses or some other way of getting information from businesses about what's happening, what their costs are. We need information from the various reporting agencies, from the banks, from the credit reporting agencies, from the victim services groups. I think we need a way to put that all together and try to relate it to the bigger problem.

[*Translation*]

Ms. Charmaine Borg: Thank you very much.

Ms. Lawson, you stated briefly that the threshold in Bill S-4 for determining whether or not there was a data breach is too high. Under this bill, it is the organizations themselves that decide whether or not to alert the commissioner or the users that there has been a loss of data or a data breach. A subjective assessment is being indicated rather than an objective assessment.

Do you have any comments on that? Do you think that could be a problem?

[*English*]

Ms. Philippa Lawson: Yes, I think that is problematic. There is a strong incentive for organizations not to report security breaches. So the law, in order to be effective, needs to address that incentive, needs to provide a counter-incentive, and I think that counter-incentive has to be an objective standard that is low enough that they will be reporting all material breaches. That was the standard in previous iterations of this bill. I'm not sure why it's been changed in Bill S-4.

It's a big issue. There are two standards here. There's one for when the organization has to report the breach to the Privacy Commissioner, which is not necessarily public, and there's an issue over whether that should be made public or not, I suppose. The other is when they are required to report it to the affected individuals.

I think it makes sense to have a lower standard for reporting breaches to the Privacy Commissioner, and a higher standard for reporting to individuals. I'm not sure why the government has seen fit to apply the high standard to both. Security safeguards are a fundamental piece of this identity theft puzzle, and organizations play a huge role in this. By establishing an objective standard under which organizations have to report security breaches to the Privacy Commissioner, we will only then have any decent registry or inventory of security breaches, of ways in which organizations are not meeting the standard for protecting personal information.

● (1205)

The Chair: Thank you, Ms. Lawson.

We're well over time for Madame Borg's turn.

We'll proceed now to the Conservatives, Mr. Laurie Hawn.

Hon. Laurie Hawn (Edmonton Centre, CPC): Thank you, Mr. Chair.

Thank you all for being here.

Mr. Fernandez, one of the hats I wear is Canadian co-chair of something called the Canada-U.S. Permanent Joint Board on Defence. Our mandate is to advise on defence and security issues for North America writ large.

One of the areas of our concern is cyber: cybersecurity, cybercrimes, cyber-espionage, cyberterrorism. When you consider all the things we do that depend on software, which is pretty much all the things that we do, the potential for shutting us down, as you said, is enormous. It was done in Estonia, in Georgia, other places.

You mentioned we are losing the battle. I don't think you were talking about this specifically, but I think you have looked at this area somewhat. Without getting into anything classified, would you say we're losing the battle there, too, and if so how can we stop losing that battle?

Dr. José Manuel Fernandez: We are losing the battle from a technological point of view indeed, not so much in terms of development of new technologies but in terms of deploying them and deploying them effectively, whether it is to combat identity theft or some other more serious issues. Again, it goes back to the fact that those who have the power to deploy those technologies are not motivated to do so. There's a broken triangle of incentives here. Those who suffer, the public, those who can suffer from identity theft, a lot of the time their machines were not hacked, it was somebody else's machine, or in the case that we were just discussing, it was the organization's.

So this is where I think government needs to show leadership and try to mend and put that triangle of incentives together so that those who can fix the problem feel the pain if they don't, or they feel the positive incentives of doing so, for example, through insurance premiums or better deals with government. The technologies are there.

Just to mention one example, when we're talking about identity theft—and the same applies for crossing the border into the U.S.—biometric technologies exist and they are affordable. Granted, they are not applicable to all applications like banking, but there's also two-factor authentication. Again, our friends in the U.S. have made it mandatory for a government-related application to have two-factor authentication for logging into government web servers.

But on the other hand, certain sectors of the industry are going the other way. The banking sector, mostly driven by profit, has decided to go back in the authentication technology and is now promulgating RFID credit cards, that are, from an authentication and identity theft point of view, a bigger problem than we had.

The technology is out there. The standards are out there. The common criteria, for example—you were talking about software of government—are a very well-written, very comprehensive set of technical standards that are being applied to highly secure government systems. Why shouldn't they be applied to certain sectors of industry as well?

Hon. Laurie Hawn: I'm told that the Chinese have about two million people working on nothing but cyber because they can probably afford to have two million people working on nothing but cyber. Obviously we can't match those kinds of numbers. You said at one point that lawmakers must lead us away from this, whatever this is. I mean, academia, industry, and so on got us there. I don't think we can pass laws that will change it. I think it obviously has to be a collaborative approach.

How do we combat this? I'm thinking more on the national security side necessarily, but there are applications everywhere. Are we teaching enough folks? Are we opening up the academia enough to get enough people qualified in these areas? I'm thinking national security, but it's equally applicable to the everyday problems that we face with identity theft, and so on.

Do we need to put more emphasis on the education area to get people qualified?

● (1210)

Dr. José Manuel Fernandez: Yes, I think it's important. Again, the United States has shamed us by investing way more money than we have, dollar for dollar, citizen per citizen, in the development of educational programs in computer security. Also I'd like to underline the fact that—as you say—the solution to this problem is not only technology. The Americans have been developing a lot of programs for training computer security experts at the technological level, but what we need is more people like the witnesses around this table who understand the problem from a social point of view, from an economic point of view, and even from a political point of view, because—as I said earlier at the end of my address—we can help find ways to close the Pandora's box, but I'm just an engineer, right? You're the politicians. We have to work together, and you have to show the way.

Hon. Laurie Hawn: You mentioned Nortel and who has taken over from Nortel, and that's no secret. That's on a commercial level. If you take that to a much higher national security level, the potential is frightening. To me, we're talking about the old—in nuclear terms—mutually assured destruction. They could basically turn us off whenever they want. They probably know we can turn them off whenever we want. It's a matter of staying one step ahead, and that goes back to data, I think.

Mr. Dupont, you talked about the problems with data. How do we get and keep better data?

Dr. Benoît Dupont: As I think has already been alluded to, one of the ways is to make the disclosure of some data held by the financial institutions...but also the retail institutions. We're talking a lot about the financial sector. The financial sector sees a lot of this identity theft happening, but the retail institutions are also responsible for the leakage of this data. They should be held responsible. They should be much more forthcoming about these types of events.

I think the government and some kind of authority within government should have the power to request that this data be made available, not necessarily...well, yes, maybe made available on a very broad basis. Someone mentioned the naming and shaming. That's what happened with the anti-theft devices on cars in the 1970s, when the insurance sectors and governments were tired of having so many cars stolen. Someone decided one day to publish the list of the 10 most stolen cars on the market. Twelve months after that, all these cars were equipped, for free for the taxpayers, with anti-theft devices.

So the automakers, who had been saying there was nothing they could do against it, suddenly found the resources and the technology to equip their cars, just because this data was made available to all the consumers to make their decisions based on the facts.

I think it's the role and the responsibility of the government to try to extract this information, not in a punitive way but in order to make this phenomenon more transparent and to make sure that consumers and citizens have all of the information. As my colleague Ms. Lawson said, there is very little that we can do as consumers, as individuals, but there is a lot that organizations can do to protect us as consumers.

Hon. Laurie Hawn: I guess that's why I don't buy a Honda Civic.

The Chair: Thank you, Mr. Hawn. That concludes your time, on that note.

Perhaps I can remind committee members and witnesses that the seven minutes is for questions and answers. If we could keep them as brief as possible, more members would have an opportunity to question.

Next, for the Liberal Party, we have my colleague Mr. Scott Andrews.

You have seven minutes, please, Scott.

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

I'd like to thank you folks for being here.

Susan, I'd like to dive into a little bit of what you mentioned near the end of your presentation, about the credit reporting agencies themselves. I think they probably can be an early warning system if someone's identity is being compromised. I think the role they play in helping consumers protect their identities is crucial. Most of us don't go looking for our credit scores or our credit history until after the fact, until after something happens.

How can we engage them? They will be witnesses here as well. What kind of questions...or how do we engage them? What kind of role do you think they could play here? Perhaps you could elaborate a little bit more on these credit reporting agencies and how they could help detect early on if someone's identity was potentially being compromised.

● (1215)

Dr. Susan Sproule: As Ms. Lawson said, the more serious type of identity theft financially is new accounts fraud. The only way you can find out if someone is opening up accounts in your name is through the credit reporting agencies.

As I said, I do a pretty good job of protecting my information as an individual. It's limited, what I can do, but I don't give out a whole lot of personal information, only what's required. I take all the advice that's given to consumers with regard to protecting my information.

One piece of advice that is often given to consumers is that you should be checking your credit report on a regular basis. I did that once about five years ago. It was such a chore to go through and collect all this information. I had to mail it off, which is very insecure. If anyone intercepts that envelope, they have everything they need to steal my identity. I sent it off to both credit reporting agencies. I got a credit report back from one. I never even received it back from the second one, which was sort of a source of concern. I ended up phoning them, and they said, “Oh, yes, we received it. Something must have happened.”

To really protect myself, I would like to go online once a quarter to get an instantaneous look at my credit report. That's something I would do to protect myself. At the moment, that costs me $24 each time I do it.

Mr. Scott Andrews: It's $16 a month.

Dr. Susan Sproule: Or I can pay $16 a month and they'll send me that and some other sort of advice about how to protect myself. It really does bother me that they're making a profit out of the problem, because then where's the incentive for them to help get rid of threats? It bothers me when my bank offers to sell me identity theft insurance. Isn't that their job, to protect my information?

Mr. Scott Andrews: Ms. Lawson, do you want to comment on the credit reporting agencies as an early warning system that someone's credit is being compromised?

Ms. Philippa Lawson: Yes, I would totally agree with your comments in that respect and I'm glad to hear they will be coming before you. I think you should be asking them a lot of questions, including why they're not offering credit freezes to Canadian consumers while they are in the United States.

There are a number of other things they could and should be doing. One has to do with credit monitoring and providing reports, as you just heard. It costs a lot of money and it's a huge effort for Canadians. We are entitled to one free report per year by mail, but the credit bureaus charge to get online access and they make it difficult and they don't always follow through.

In the United States, there's a requirement for one-stop shopping. There are three credit bureaus in the States. In Canada, there are two. It would be helpful if consumers—particularly for victims of identity theft—if you could go to one central source and get the reports from both agencies. That would be helpful.

I think you should be allowed to access your report online, at no fee or a very low fee, and get credit monitoring services for no or a low fee, particularly if you can show that you may have been a victim of fraud. It's interesting that in the United States there are laws under the Fair Credit Reporting Act that we don't have in Canada, other than very general principles in our data protection law. For example, in the United States credit bureaus have to block reporting of information where the consumer provides evidence of fraud. They have to notify furnishers of allegedly fraudulent information, once they've been notified by the victim that there appears to have been a fraud.

These kinds of very specific obligations on credit bureaus can really help to prevent, detect, and deal with the problems of identity theft.

Mr. Scott Andrews: Back to you, Susan, you mentioned early on that those committing identity theft are not the ones committing the identity fraud. I wonder if you could elaborate on that a little bit. Is there a way that law enforcement and people could stop the in-between of when identity theft happens to when the fraud occurs?

● (1220)

Dr. Susan Sproule: I guess there are different kinds of identity theft. Some is very opportunistic and targeted, where someone has access to the information, gets the information, and then impersonates that person to commit a fraud. In that case the thief and the fraudster are the same.

When we're talking about data breaches, where hackers go in and get into databases and collect information, that information goes into black-market marketplaces and is sold. There are academic studies that have looked at the black market and what a credit card account identity is worth—what an identity, something that has your social insurance number and your mother's maiden name, is worth. So you can get data on that from these black markets, and that's the gap between the theft and the fraud. The fraudsters go and—

Mr. Scott Andrews: Mr. Fernandez, do you want to jump in on that as well?

Dr. José Manuel Fernandez: Yes. The problem is that, unfortunately, a lot of these identity thieves are not in Canada. They're not within our jurisdiction. It's organized crime in eastern Europe, in Indonesia, in Brazil, and they're simply outside our jurisdiction. A lot of these countries are not collaborating with law enforcement in Canada. That's why the Convention on Cybercrime that we still need to ratify is important.

Mr. Scott Andrews: How about the issue of the black market? Is there a way that law enforcement can zoom in on that, or is it something that's out there and they can't—

Dr. José Manuel Fernandez: I'm going to forward that question to my colleague, Benoît Dupont, who has some interesting ideas about what we could do about disrupting the black market.

The Chair: If we could have a very brief answer please, Mr. Dupont. We're almost out of time.

Dr. Benoît Dupont: A very brief answer.... I think so far the only country that has really made some investigative investments in trying to disrupt the black market is the United States with the U.S. Secret Service. There is no reason why the RCMP, which is able to leverage large sums of money to conduct large investigations on the mafia.... You know, the Colisée investigation in Quebec cost about $30 million. So there is no reason why the RCMP couldn't invest this type, or maybe smaller amounts of money, to try to disrupt black markets. It has a network of liaison attachés all across the world who try to cooperate. But so far, only the U.S. government has invested this type of money to investigate these types of crimes outside its borders.

The Chair: Thank you, Mr. Dupont.

Thank you, Mr. Andrews.

Next for the Conservatives is Mr. Zimmer.

Mr. Bob Zimmer (Prince George—Peace River, CPC): Thank you all for coming to committee today. I think a lot of us who spend a lot of time on the web are concerned about how secure our information is.

I have a few questions on some basic information. How is the $3 billion quantified? I think somebody used that number as the amount that is affecting Canadians and how much the loss is. How do you quantify that amount?

Dr. José Manuel Fernandez: That figure comes from Symantec, which is an anti-virus company. The 2013 report for Canada reports that figure.

I'm not an expert on how to quantify these things. Some people might say they suspect that figure comes from a party that is interested in maybe growing the size of the problem, but that's probably better answered by some of my colleagues here who actually are specialized in those numbers.

Mr. Bob Zimmer: Does anybody else want to respond to that quickly? I have more questions, but if somebody could answer that....

The Chair: Dr. Sproule, would you like to go first?

Dr. Susan Sproule: Just as an example, and it's old data, but when we did our survey of consumers in 2008, we found 1.7 million people or 6.5% of Canadian adults were the victim of some kind of identity fraud in the last year. They spent over 20 million hours and more than $150 million to resolve problems associated with those frauds. That's just the consumers' out-of-pocket costs, which is a small part of the big problem.

Mr. Bob Zimmer: That's significant. Thanks for that.

I would ask you another one. I have a couple more simple ones.

We have all had a typical virus on a computer. I'm assuming everybody has where the sound stops working for instance, or something stops working. I guess I need to get a better understanding of who the people are. Are we dealing with the high schooler who wants to just turn my sound off on a computer? Are they getting other information off my computer that's more important than that, and that's just a residual effect?

We always think about the big guys, and the Chinese, or whoever it is that has a full frontage attack on our information, but maybe take us through the different levels of how this is done.

● (1225)

Dr. José Manuel Fernandez: Yes, I will very briefly.

The world of cybercrime has become more complex in the last few years. There are at least four different kinds of groups. There are those who attract you to a website where you are going to get infected. There are those who operate those websites to infect you when actually they are sending in the viruses, but they don't hold your machine. Then they sell your machine to somebody who's going to be operating that machine for several weeks or months. Then those button operators as we call them will rent those machines out to the people making the money and making the fraud. They will use those infected machines to send spam. They might mine your machine for financial data. That's one of the ways of doing identity theft. They might use that machine to conduct a denial of service attack on some country.

There are many ways in which these infected machines can be monetized. That's why when I say it's all the same problem it's because that same arsenal of infected machines can be used for cyber-espionage, cybersabotage, identity theft, and mass market cybercrime. All of these groups are collaborating. They used to be doing it just for fun, then they were doing it for money, but what we have seen is that they are also using it for political gain and for propaganda as well.

Mr. Bob Zimmer: I have another question as a follow up to that.

You talked about the one company that had to replace 30,000 computers. Is that a correct amount?

Dr. José Manuel Fernandez: That was Aramco. Yes. They had about 30,000 desktops that were—

Mr. Bob Zimmer: It was always my understanding that a virus would only have done so much hard damage to a computer, but it sounds like this particular virus or whatever happened there had much more of a direct effect on the actual hardware. Can you explain that?

Dr. José Manuel Fernandez: Yes. Typically viruses do not harm the hardware, but in this case it was a management decision of Aramco. Of course they are rich. They said the best way to deal with the problem is to throw away all those computers, buy new ones, and reinstall them.

Probably that was a very good decision because it's probably cheaper to do that than to have to reinstall them from scratch. Do the math, $1,000 a machine. That's a big number.

Mr. Bob Zimmer: Again just to get back, we talked about different levels of where this is at, and you talked about espionage.

Is the sound not working on a particular computer evidence of something worse, or is it a kid hacking from a high school computer just to tick people off?

Dr. José Manuel Fernandez: As I said, high school kids hacking with respect to the Heartbleed incident, students from the University of Western Ontario, they used to be the bigger problem. Now they are just a nuisance. They are not the problem.

From a social-political point of view, however, in countries where there hasn't been much of an IT economy developing, you have all of those whiz kids who instead of finding jobs in Kanata or Silicon Valley go into cybercrime. They have become professional, and they have people with big guns and big muscle who are making sure they do what they need to do.

Mr. Bob Zimmer: Thanks. That's all I had.

Thank you.

The Chair: Thank you, Mr. Zimmer.

We will move on to five-minute rounds for questions and answers.

Mathieu Ravignat, go ahead for five minutes, please.

Mr. Mathieu Ravignat (Pontiac, NDP): Mr. Fernandez, to come on the tail of what my colleague there said about Heartbleed, at the beginning of your presentation you said that the government infrastructure is—I think “pitiful” was the term you used or it may have been something rather colourful, which gets me worried.

What decisions have we been making in the last few years that has led to the current situation we find ourselves in?

Secondly, what needs to be done?

Dr. José Manuel Fernandez: It's not only the government. It's Canadian industry. It's foreign governments worldwide. It's a worldwide problem. I don't think the Canadian government is less diligent than all the governments worldwide or even all the big organizations. It's not only in the last few years. It's in the last 30 years. In the sixties, seventies, and eighties, the IT industry was a well-dominated, organized market. It used to be IBM and a few other people. It was well understood how it worked, and whose throat you had to choke if there was a problem.

But with the arrival of the web, then it became a free-for-all. Anybody who had some kind of coding knowledge could develop a web app. Anybody who could contribute to the development of open-source software could, and the standards we were used to were dropped because it was new, it was shiny, and we wanted to have the cool stuff and we wanted to make a buck as quickly as we could with it. The banks are a good example of that, right? The fabulous profits they made in 2000 were due to that.

The government just followed suit. They did what everybody else did in adopting technology, but they abandoned the standards they had in the previous world. In the mainframe world, there were standards about development and so forth, but when we went to the new paradigm of client, server, and web, we just forgot it. We just abandoned it completely. We need to go back.

● (1230)

Dr. Susan Sproule: When we talk about technology, we talk about security, and data security is the weakest-link problem. There are technological aspects to it. We can have good technology. We have encryption technology, but it's just not being used. People don't use it. When we get into new types of information like health information and electronic health records and the way that this is now being transferred among all these different networks and systems, the fact that we have data breaches of health information that's not encrypted is criminal. That shouldn't happen. But that's a people-problem not a technology-problem. The technology is there.

Mr. Mathieu Ravignat: The technology is there but the public policy isn't.

Dr. Susan Sproule: Yes, with encryption, the policies may even be there, but you have to have people to actually do it.

Mr. Mathieu Ravignat: Right.

The Chair: Mr. Ravignat, we could invite some of our remote witnesses to see if they want to take part as well.

Mr. Mathieu Ravignat: Certainly.

The Chair: Do either of you have a comment on Mr. Ravignat's last comments?

No. Fair enough. Okay. I wanted to make sure you were included. Thank you.

Mr. Mathieu Ravignat: My next question is on the recent development of payWave technology. These are cards that you can just tap to pay, and it seems like there are a number of security issues surrounding that technology, particularly credit cards, banks, and so forth.

Mr. Fernandez, you were part of a research project that looked at this. Do you have any results from that research, anything helpful to show us?

Dr. José Manuel Fernandez: If you don't mind, I can borrow your credit card, I'll shut off my phone and I'll be able to read your credit card number over the air, and your name, and your expiry date. There's an app for that.

Mr. Mathieu Ravignat: Given that this is a public session, I'd rather not go through that exercise.

Voices: Oh, oh.

Dr. José Manuel Fernandez: Yes, unfortunately the banks were mostly motivated by profit in developing this technology. They wanted to get their filthy 3.5% of profit on the market of the small pocket change.

That's at the cost of Canadians' privacy because that technology is not protecting their privacy. If I steal your credit card from your wallet, you'll probably notice because I have to put my hand in your pocket at some point, but with this new technology I don't even have to do that. I only have to get close to you in the metro, on the subway, or within 10 centimetres, and that's it; I've stolen your credit card credentials and I can make transactions on it. The technology that they themselves have created could prevent that, but they've deployed it in a mode that is less secure, for the time being, because they don't want to have to invest the money required to change the infrastructure for the payment terminals.

Mr. Mathieu Ravignat: Regulation hasn't caught up, I imagine.

Dr. José Manuel Fernandez: What regulation...?

Mr. Mathieu Ravignat: Okay, right. That's a problem in and of itself.

The Chair: Time is pretty well up, Mr. Ravignat. Again, is there anybody else who would like to remark on that last topic? We'll give an extra minute or so.

Ms. Lawson.

Ms. Philippa Lawson: Chair, I'd just like to make one point on that. I think it can be helpful to separate two different categories of identity fraud here. First are these mass market credit cards where the industry has basically made a decision to risk more fraud in exchange for more transactions. The cost of that is borne by consumers in the broad base of consumers through higher interest rates and fees, as Susan Sproule said earlier. As long as the individual consumer is being reimbursed by the financial agency and not held liable for the fraud, it doesn't have the same impact as the kind of individual identity theft and fraud where the individual victim does have to deal with all of the financial fallout.

● (1235)

The Chair: Thank you.

One final comment....

Dr. José Manuel Fernandez: It's actually worse than that because if the banks are paying, we could say it's a zero sum game. Whatever I lose, I gain back. The problem with this technology is that they actually present a threat to our privacy like we've never seen before. We cannot turn off these cards. They're not only transmitting what you're paying, they're always on. A store could set up a detector of these cards, and they would know that you are the same guy who came two weeks before to buy that hat, or that you are the lady who came the day before to ask for that fur coat, whatever. This could be done not only for marketing purposes but for tracking purposes, stalking purposes, even security breaches.

They've created a problem that is much bigger than the one concerning Internet banking fraud.

The Chair: Thank you, Dr. Sproule.

I thought I'd go a little longer because it was the first we heard of that very interesting subject, but Chad, our clerk, just reminds me that he keeps his card in a kryptonite sleeve or something so nobody can access it.

Next for the Conservatives is Tilly O'Neill Gordon.

You have five minutes, please, Tilly.

Mrs. Tilly O'Neill Gordon (Miramichi, CPC): Thank you, Mr. Chair.

First of all, I want to thank all of you for the time you're spending with us and giving us such valuable information. We were all very aware of the Heartbleed bug, which caused quite a problem. You mentioned that this led to the unauthorized disclosure of at least 900 social insurance numbers.

I wondered, are these victims aware that their numbers have been disclosed? Would you say most victims of identity theft do become aware that they have been targeted?

Dr. José Manuel Fernandez: With respect to the Heartbleed incident, the press release from the CRA was that those whose numbers had been identified would be notified by mail. I believe they will do that.

In more general terms, the answer is no. From data that we've compiled over the years by penetrating black markets and also by compiling statistics of infection and so forth, we believe that for every victim of identify fraud, for every account emptied, there are probably 10 times as many that have been compromised. Fraud prevention measures of the banks are preventing cybercriminals from emptying more accounts but the criminals have a reserve of 10 times more accounts than they need, with a capacity to empty them out right now. There are many more victims of identify theft than there are of fraud. They just haven't been defrauded yet.

Mrs. Tilly O'Neill Gordon: Do you have something to say?

Dr. Susan Sproule: No. I would agree with that.

Mrs. Tilly O'Neill Gordon: The other thing I was thinking about is, what is the follow-up on these victims? Do they receive any support? How is the follow-up for them?

Dr. Susan Sproule: That'll be Pippa's question.

Ms. Philippa Lawson: I have no idea what's being done by the organizations that suffered from Heartbleed in terms of proactive reaching out to victims. This is why security breach notification laws are so important. They would require exactly what you are suggesting. They would require notification to those victims, so that they could take the precautions to shut down accounts and protect themselves against fraud.

A very important point was made earlier. The fraud could happen years later. In fact, there is a growing category of identity fraud in the United States right now involving children, where the fraudsters get hold of young children's social security numbers.

If you choose and some parents do choose to get social insurance numbers at the time of birth—you can for your children—so that they can register them for educational savings plans or whatever. Once you do that it becomes susceptible to identity theft. Someone might not realize until they're 18 years old and they go to get their first job or file their first income tax return that they have been a victim of identity fraud for years on the basis of this previously issued information.

This problem of a lag between the theft and the fraud can be very significant.

● (1240)

Dr. Benoît Dupont: If I may add a few words. In the survey we conducted in 2007 in Quebec, we had a few questions about the level of satisfaction regarding the number of institutions that had dealt with victims. Among the victims of identity theft, the levels of satisfaction were much higher toward banks than toward the police.

I know the bank lobby is here, but I'm saying that we also have to rethink the way that police organizations deal with the victims of identity theft because for many police officers this is not a real crime. This is absolutely false because we know that it can also not only have financial but psychological implications for victims.

Although they are more responsible, the banks are doing a better job than the police in dealing with victims. We also have to maybe understand how we could make victims feel more welcome and treated better than they are currently.

Mrs. Tilly O'Neill Gordon: I know we've covered lots of ideas on this, but I'm wondering.... You referred to changes that we've made on world safety and to cards over the years. Of course, we're going to have to hopefully see the same thing happen. If you were to see one big change that you'd like implemented right away, do you have one that you'd like to see implemented?

Dr. José Manuel Fernandez: It's education, user education. There has been talk about the Internet driving licence. I don't think we want to necessarily restrict access to the Internet, but the government should take leadership in providing or even having some mandated educational programs for children or for adults. I understand that some of this is provincial jurisdiction, but definitely the federal government can provide leadership by providing the content.

This is probably where you're going to find less resistance. Nobody is going to say no to education. This is a good opportunity for leadership.

If you're saying let's enact some law that's going to require some standard enforcement, you will find resistance from the private sector, but at least let's get the easy win and that's education.

The Vice-Chair (Mrs. Patricia Davidson (Sarnia—Lambton, CPC)): We'll now go to Madame Borg, for five minutes.

[*Translation*]

Ms. Charmaine Borg: Thank you.

My question is for Ms. Lawson because she commented briefly on Bill S-4. However, if other witnesses also have any comments to make I would be happy to listen to them.

Do you think that Bill S-4 represents everything that should have been done to make sure that our privacy legislation is up to date and protects Canadians against these risks in this day and age? Should anything be added to the bill? Does anything not go far enough or is there anything that shouldn't be in the bill?

[*English*]

Ms. Philippa Lawson: I've already mentioned the breach notification provisions which can be improved, in my view. I haven't yet done a thorough review of it, but certainly, the area of enforcement, as I mentioned in my comments, is one where I think there could be more that could be done to, for example, give the Privacy Commissioner more enforcement powers herself, or to allow private individuals to hold organizations accountable for non-compliance with their data protection obligations under the act.

[*Translation*]

Ms. Charmaine Borg: Thank you very much.

Does anyone else have something to add?

Mr. José Manuel Fernandez: Yes.

When there is a data breach it is important that not only the users be notified. There also has to be an analysis. However, an analysis can sometimes mean that police services or government or organizations will be investigating the incident and identifying the causes, whether they be technological causes or a lack of procedural diligence.

The goal is not necessarily to punish those who are responsible but rather to learn from the incident. We have to make sure that as a government and a society we are moving towards better practices, the most effective practices.

Ms. Charmaine Borg: Thank you very much.

Ms. Sproule, you said that organizations that have information on an individual's identity have a certain amount of responsibility in terms of protecting that information. Obviously the government is one of those organizations because it has an enormous amount of information about Canadians. Recently the Heartbleed bug compromised personal data. I would therefore like to move the following motion:

> That, as part of the study of the growing problem of identity theft and its economic impact, and pursuant to Standing Order 108(3)(h)(iv), the committee invite the Interim Privacy Commissioner of Canada to discuss the Heartbleed bug and its repercussions on all affected federal departments.

I think that it would be important to include this in this study given that this is a very recent event. We have several questions about this. A few committee members have even asked some of them. I would also suggest to the committee that we might also want to invite Canada Revenue Agency officials back.

I believe I have reached the end of my time. Have I?

● (1245)

[*English*]

The Vice-Chair (Mrs. Patricia Davidson): You have another minute and a half.

[*Translation*]

Ms. Charmaine Borg: I will therefore use it.

I apologize for tabling this motion during testimony. Unfortunately that's the way we have to work in this committee.

I have a last question I would like to ask and it is somewhat related to the motion that I have just moved. Do you think that the federal government and all its departments is ensuring sufficient protection of our personal information?

[*English*]

The Vice-Chair (Mrs. Patricia Davidson): Excuse me for a moment. Sorry to interrupt. Are you just giving notice of motion, or are you tabling it for debate right now?

Ms. Charmaine Borg: I don't think it would be appropriate to debate it while we're still questioning our witnesses.

The Vice-Chair (Mrs. Patricia Davidson): That's fine. I just needed to clarify that.

Ms. Charmaine Borg: Okay, thank you.

Mr. Paul Calandra (Oak Ridges—Markham, CPC): Madam Chair, I'm prepared to debate it if she's prepared to debate it. I request that we move in camera to debate the motion.

The Vice-Chair (Mrs. Patricia Davidson): We have a motion to go in camera, which is not debatable.

Mr. Paul Calandra: It's a motion to move in camera so I'd like to thank the witnesses for coming.

The Vice-Chair (Mrs. Patricia Davidson): A recorded vote has been called.

(Motion agreed to: yeas 4; nays 3)

The Vice-Chair (Mrs. Patricia Davidson): We will pause for a couple of minutes as we move in camera. Before we do that I want to thank all of our witnesses today. It's certainly been a very interesting presentation that we've had from all four, and we thank you for that. It's given us a bit of a different perspective, I believe, on some of the testimony that we've heard. So thank you very much for your time.

[*Proceedings continue in camera*]