House of Commons
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 045 • 1st SESSION • 39th PARLIAMENT

EVIDENCE

Tuesday, May 8, 2007

Chair

Mr. Tom Wappel

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, May 8, 2007

● (0905)

[*English*]

The Vice-Chair (Mr. David Tilson (Dufferin—Caledon, CPC)): Good morning. This is the Standing Committee on Access to Information, Privacy and Ethics, meeting number 45, on Tuesday May 8, 2007.

The order of the day, pursuant to Standing Order 108(2), is a study on the topic of identity theft.

We have before us today, from the Office of the Privacy Commissioner of Canada, Jennifer Stoddart, the Privacy Commissioner; Wayne Watson, who is the director general, investigation and inquiries branch; Carman Baggaley, who is the senior strategic policy analyst; Steve Johnston, who is the senior security and technology adviser; and Lisa Campbell, who is the assistant general counsel.

Commissioner, you have brought quite a force with you today; these are pretty impressive names. We do appreciate that. You're our first group of witnesses on this topic, which the committee thinks is very important. Thank you very much for coming.

Please commence your presentation, and we will allow time for questions from the members of the committee. Thank you very much.

Ms. Jennifer Stoddart (Privacy Commissioner, Office of the Privacy Commissioner of Canada): Thank you very much, Mr. Chairman, for that welcome.

I'd like to begin by congratulating this committee for choosing to hold hearings on the very crucial issue of identity theft. As you have sensed—rightly—many Canadians not only are victims of identity theft, they are very anxious about what the government is going to do to combat it.

As this is, as you mentioned, Mr. Chairman, the initial session of your series of hearings, I brought quite a few people from my office who have specific expertise.

With your permission, I'll make a brief presentation. I think all the honourable members have a reference book that we've prepared for them.

The Vice-Chair (Mr. David Tilson): Yes. We do have that brief, Commissioner.

Ms. Jennifer Stoddart: Our submission is found at table 2, section 2. There is quite a bit of material that I thought would be useful, either today or when you're looking at subsequent testimony.

The Vice-Chair (Mr. David Tilson): Excuse me, Commissioner. Obviously the ladies and gentlemen before us have a certain expertise. I have introduced them with their titles, but perhaps you could elaborate on what they have to offer so questions might be directed to them.

Ms. Jennifer Stoddart: Thank you very much, Mr. Chairman. I will do that.

I have two staff members, Valerie Akujobi and Johanne Séguin, who have prepared the overview.

Lisa Campbell is the assistant general counsel. She has worked as a criminal defence lawyer and has quite a background in criminal law. We thought that would be useful for the members because of the implications of modifications and applications of the Criminal Code.

Carman Baggaley has an extensive background in communications policy throughout the government, from different points of view.

Wayne Watson joined our staff last year. We're very happy to have him. In his previous incarnation, as they say, he was assistant chief superintendent in charge of white collar crime at the RCMP. I think he could answer your questions in a depth that I wouldn't be able to.

Steve Johnston, our chief technology and security adviser, is an engineer and has an extensive background working for the Canadian government in communications and security. He can answer all your technical questions.

As an introduction to the session then,

[*Translation*]

we're obviously talking about privacy and identity theft here.

I think it's appropriate to start by reminding ourselves that identity theft is one of the very serious privacy offences. These days, individuals must have control over their identity and over all the aspects that constitute it. That is central to their ability to participate in a democratic society and to enjoy government, financial and community services.

So as Privacy Commissioner, I consider identity theft one of the very serious invasions of privacy.

● (0910)

[*English*]

It has been said that identity theft is the ultimate privacy transgression. Unfortunately more and more Canadians and people worldwide are subjected to this privacy violation.

One of the things you'll see in our paper is that identity theft is hard to define. There's no one clear definition. I think that's one of the challenges we have when trying to come to grips with it. It certainly seems to cover the phenomenon of fraud. It covers the act of taking information from someone without their consent; but of course taking information from someone without their consent is not necessarily a criminal violation. It may be a violation of PIPEDA; however, as I understand it, until you do something with it, the law does not apply. So this is one of the challenges we have in trying to control it. The issue of intent and the issue of use are integral parts of identity theft.

With a definition that is flexible, there isn't a reliable series of statistics. We can give you various statistics. There are American, Canadian, and European statistics. We've given you here Canadian statistics for the year 2006. They're pretty impressive if you consider that $6 million of losses were reported to PhoneBusters, which is a police network run primarily by the Ontario police, the OPP.

ID thieves obtain information in many ways. I would refer you to the excellent paper that CPIC did. I think CPIC is appearing before you concerning all the ways ingenious wrongdoers can obtain your personal information. We've broken those down into three here: physical, technological, and what's called social engineering. These are the main ways in which information is obtained. Theft of your ID, theft of documents—this includes the usual phenomenon of stolen laptops, which happens throughout the public and private sector.

Unfortunately, in physical theft there is an increasingly recognized phenomenon of employee theft, insider theft, using people called moles. In French, *on les appelle les taupes*. These are people who, either for personal reasons or for financial reasons—because they're paid—pass inside information to outsiders. This is not a new phenomenon, but it seems to be accentuated, and both of the data spills that we're currently investigating—and Mr. Watson can talk to those—seem to have been precipitated by different kinds of insider wrongdoing.

In that group, too, I would put what's known as dumpster diving. This involves companies that don't shred or dispose of their personal information appropriately, and then people with a lot of initiative go through the dumpsters. I remember last year my fellow commissioner, Commissioner Frank Work of Alberta, was so exasperated by what reporters were finding in the dumpsters in Edmonton that he said the next person he was going to hire for his staff was a dumpster diver to police the dumpsters of the city, to make sure they got all the personal information before the ID thieves did.

With regard to technology, hacking into databases is increasing. Then there's the whole issue of spyware and malware—which Mr. Johnston can talk about—often carried by spam.

Finally, there is social engineering. That is something, unfortunately, with which I have some direct experience. This is passing oneself off as the real customer in order to get the customer's confidential information, for example, phone records kept with the telephone companies.

Bogus contests encourage people, and perhaps part of our population increasingly finds it difficult to distinguish the real contests from the bogus contests. I'm thinking about seniors. I'm thinking about people who perhaps are not following developments on the Internet for various reasons, and they can fall prey to this.

● (0915)

In our submission to you, Mr. Chairman, we are taking the position that this problem requires not only a global approach but also strong centralized, coordinated leadership to try to be effective in combating ID theft. We refer you to the American approach—and you have the conclusions of the presidential committee that was struck last year at the request of President Bush. It just brought down its report about two or three weeks ago. We have given you a copy of the conclusions of that report in your binder.

We'd also draw to your attention the Federal Trade Commission's identity theft data clearing house, which is a central place to report the phenomenon of identity theft, in order to understand its contours and its functioning a bit better.

[*Translation*]

What is the role of the Personal Information Protection and Electronic Documents Act, and is it adequate to counter identity theft?

PIPEDA is not a tool that, alone,enables us to combat this phenomenon. However, since it came into force six years ago, it has raised the standards of industry and commerce in Canada. In particular, it imposes restrictions on information gathering. The safeguard principle permits the secure and confidential holding of personal information. It also makes it possible to limit the time during which information may be kept, as well as the number of persons who have access to it.

In your recent report, you referred to notification of data breach. You also mentioned the extent to which such a standard was essential in the act. In cooperation with the industry, we are currently developing guidelines, pending amendments to the act.

Last fall, we established guidelines on what we call authentication. These are standards whose purpose is to enable us to allow a person to certify who he or she really is. For example, when we call the telephone company to obtain information on telephone calls, we have to prove to the company who we are. There are various type of authentication. Mr. Johnston can tell you about the standards suggested in the guidelines.

We also conducted an investigation into a number of complaints that were brought to our attention. Those investigations, I believe, have helped raise standards, particularly in the banking industry. Among other things, I'm talking about practices of sending unsolicited credit cards bearing the names of people. I believe that is a practice that disappeared a few years ago. We're also trying to investigate the practice of sending cheques accompanied by an offer of credit, if they are used, without people having requested them.

[*English*]

What are some of the legal sanctions that we could think of? Personally, I think we have to look at a range of measures. I don't think it's just an issue of the Criminal Code. As you know, our law administrators hesitate to use the Criminal Code: the standards of proof are higher, and the charter may apply, and so very often you have to have a fairly clear-cut case to use the Criminal Code.

That's why I think we should look at civil sanctions that are very easy to prove and easy for citizens, for example, to take to small claims courts, which may provide a more easily accessible deterrent to the growing industry of ID theft. This means, of course, that I think the federal government has to work closely with the provinces, because a lot of what happens in terms of ID theft falls within provincial jurisdiction. I think we've all heard about people in various provinces across Canada who have had their houses sold out from underneath them. This is something that basically falls within provincial jurisdiction—and I know you're going to hear from the provincial commissioners on this.

Pretexting is one of the most important ways that personal information is obtained, and it points to the fact that we need to know more about the ID theft industry: how does this work, who's making a profit from it, what is the network, who is helping it, and who is creating the demand for this illicitly obtained personal information?

My colleague the U.K. commissioner brought out a shocking report, quite frankly, on the personal information industry in the United Kingdom. We don't think those exact phenomena are in Canada, but I think the report is well worth reading. He has called for criminal sanctions and has, I think, successfully sued some of those who are in the industry of obtaining illegal personal information.

More recently here in Canada, there was a consumer report this winter on a Radio-Canada program called *La Facture*, documenting how in Canada's own financial industry there are moles working who are willing to sell information to a reporter posing as somebody in the personal information industry. We're following up on that, of course.

Not only is identity theft carried out in person, it's also increasingly carried out online. Some of the most common threats to your ID online include phishing. You have all received fake letters —and these are getting better and better—purporting to be from, or looking like they are from, your local bank and asking that you check your account numbers, and so on, because there has been a "problem". These are getting more and more realistic, and again, I think there is a whole group of Canadians who are very vulnerable to them. And for all of us, it's getting harder and harder to distinguish the real from the false.

There is something called botnets. These are networks of computers that have been turned into robots at the service of a mastermind behind a criminal racket.

Trojans and worms are implanted in our computers to make them do things we can only guess at, and don't know, but which are in aid of more ID theft and fraud.

And then there is the phenomenon among young people of what one expert has called—and this is not my term—cyber exhibitionism, the latest form of socializing online at Facebook and MySpace, and so on. This means that increasing numbers of young people have all of their personal information spread over networks.

This has direct implications too for the Government of Canada, as we move to providing more and more services online through Service Canada, not just income tax but also our pensions, our queries, our veterans pensions, and so on. The threat of receiving false messages and having this network infected, I think, is rising.

You may have noticed in January, I think, there was a false message from the "Canada Revenue Agency", or a false "Canada Revenue Agency" message, asking citizens to communicate with that agency. This was a fake message, but it looked remarkably like the real ones coming from Revenue Canada.

● (0920)

This could threaten online banking, and an increasing number of people do online banking.

So what can we do to prevent it? What is my office doing to prevent this?

Here we go not only to our investigation of complaints, but increasingly to public education. This committee has often stressed the importance of our role in public education. And you can see that we have a whole series of specialized brochures, fact sheets, and so on, that are reproduced for you in the binder. That's the information available to the public on our website.

We participated with the RCMP and the Competition Bureau in March—fraud prevention month—as well as with more than 20 other partners in a joint public education campaign. We stress the growing importance of encryption of personal information passing over the Internet. I was happy to see that you called for information destruction in your report on PIPEDA. That is implicitly part of the act, but I agree with you that we should make it more explicit, as too much information is just thrown away where enterprising people can find it.

To conclude, Mr. Chairman, I think we need clear leadership, the type of leadership that I'm sure this kind of committee could define. There's a federal-provincial task force on this to focus our ideas. They're setting up a clearing house with all jurisdictions. What is important is to get all the players together. It's not only the federal government; the provincial governments are extremely important. The police, federal and provincial, play a very important role. Those who prosecute—or can't prosecute, for lack of the tools—the people perpetrating ID theft have to be involved in this too.

I think we have to have the will to define and document this problem, and to find not just one magic bullet but the range of weapons, if I can use that terminology, in all the various areas—I've put some of them down there—ncluding the international area. We are being preyed on by folks across the border. Canada, as I have already pointed out to you, is the home, for example, of malicious spam that attacks people worldwide. So we have to cooperate with our neighbours and our trading partners on that.

Those, Mr. Chairman and honourable members, are the highlights of our presentation. I've brought all of these experts along to help me answer the questions you may have.

● (0925)

The Vice-Chair (Mr. David Tilson): Thank you, Commissioner.

Your introduction to this topic makes me even more alarmed than I was before, so I thank you for that. And I thank you for preparing this book, which we will use as research. Someone has taken a great deal of time to prepare it, and I thank you kindly.

As you know, we go in rounds for each caucus. The first round is seven minutes each, including the questions and the answers.

Mr. Pearson.

Mr. Glen Pearson (London North Centre, Lib.): Thank you, Mr. Chair.

It's nice to see you again, Commissioner. Thank you very much for coming.

Part of the thing we worry about is that, as we understand from the various testimonies we've had, things are mushrooming. It's difficult to get a handle on it. One of the things that we have to weigh, though, is that we don't want to have the kind of approach that's going to be too heavy-handed, because we don't understand fully what the problem is yet.

Now, you said that it's hard to define. And I understand that. I'm wondering if you can help us to understand. For instance, in the case of identity theft, do you keep facts, figures, and statistics about how many people have actually been charged with identity theft, how many have been prosecuted? Do you have that kind of information?

Ms. Jennifer Stoddart: No, we don't. At the OPC we don't keep that kind of information. And I'm not sure that it's kept in a systematic way throughout Canada.

Could I ask our lawyer on the staff to tell you about the kind of information that is available on who is charged?

Mr. Glen Pearson: Sure.

Mrs. Lisa Campbell (Senior Legal Counsel, Office of the Privacy Commissioner of Canada): Good morning, Mr. Pearson.

Thank you for the question. It's a good one.

I think the commissioner said at the beginning as well that identity theft isn't well defined. It can range from someone taking your credit card number to wholesale misappropriation of your identity and impersonation.

The existing Criminal Code offences were in the main written when we were thinking about traditional notions of property. The problem for the fit with identity theft is that personal information, in and of itself, isn't valued as property. The difficulty when trying to apply the Criminal Code provisions is that unless you can show a direct causal link to economic loss or some other serious disadvantage, it's very hard to prove that someone has committed an offence—what we think of as identify theft.

There haven't been reported cases, that we're aware of, of identity theft per se. However, many people have been charged under the existing Criminal Code provisions. There are at least 12 that are used in the main, but other people have suggested about 40 that can apply to theft or fraud situations, conspiracy to commit fraud. But again, that's when the personal information is used. There are no offences in the Criminal Code that target simply possessing and collecting personal information.

Does that answer your question?

Mr. Glen Pearson: It does. It's very interesting, because we're trying to strike a balance here as a committee, obviously, but what we actually don't have are the facts.

I notice in your conclusions you said that one of the things we have to do is define and document the problem. Can I ask you how you could see doing that? I'm sure you work with various agencies to do that. Would you have a national database? How would you do that?

● (0930)

Ms. Jennifer Stoddart: I think, first of all, Mr. Chairman, that you have to set up the appropriate organizational framework. The government either tasks one agency to take the lead or sets up some kind of light, temporary structure that can coordinate federal-provincial organizations, and then within that new organizational structure you define what you're going to collect and what you're going to report on. I think you have to have the means first and then start to collect the information in some kind of systematic way so that it can make sense more rapidly.

Mr. Glen Pearson: Do you have any suggestions as to who would take the lead in that, who you would think would be best suited?

Ms. Jennifer Stoddart: I did have the privilege of meeting the Minister of Justice last week. In fact, right after I appeared before you the last time, I suggested to him that this might be something that he could do: call up a federal-provincial task force with participation from all the key players and set up a coordinating structure in which all the various organizations can play a part.

Mr. Glen Pearson: One of the things people keep throwing out is the idea of a national identity card, something like that, a biometric kind of card; we hear about that for border crossings and so forth. I'd be interested in your view of that. Also, how do we monitor that? That, to me, seems to be very difficult, and I know it seems like it's a tell-all solution for everything. Do you have a view on that?

Ms. Jennifer Stoddart: Yes. My office has always been very critical of the idea of developing a national identity card because you can see, just from the short presentation, that if we can't keep control of the very disparate, fairly soft kinds of identity we have, I don't think—among other things, apart from the freedom and civil liberties implications—that we are ready to go to much stronger kinds of identity, because we don't know how to protect that kind of identity. I'm sure that at some point Mr. Johnston can speak in greater detail to that.

The stronger the forms of identification of individuals you have, the greater you run the risk of huge problems if those identities then are stolen. If my driver's licence is stolen now, I can still get another one; I can prove who I am at the bank, and this may not affect my passport, for example. But as you go to stronger forms of identity, and your identity is taken over by somebody else, you may have a real problem in proving you are who you are.

Mr. Glen Pearson: Right.

Thank you, Mr. Chair.

The Vice-Chair (Mr. David Tilson): Madam Lavallée.

[*Translation*]

Mrs. Carole Lavallée (Saint-Bruno—Saint-Hubert, BQ): Thank you very much, Mr. Chairman.

First, I'd like to thank our guest, Ms. Stoddart, and her colleagues, for being here this morning. The subject is fascinating, but I'll come back to that.

Please excuse me, but this is the only time I have, under our rules of procedure, to raise a logistical problem. So I apologize to our guests.

Mr. Chairman, the clerk told me earlier, before the meeting, that this was the only moment I had to request a change to the agenda. As you know, I announced it last week, I would have liked us to talk about the important motion that I introduced more than a week ago now concerning the internal report of the Department of Foreign Affairs on what is going on in Afghanistan. So I would really like to make this change to the agenda so that we can talk about it at the start of the meeting. Unfortunately, the clerk told me that that was not possible.

After speaking with my colleagues, particularly Mr. Wallace, we agreed together that, if you assure me that we can take half an hour at the end of the meeting to debate this motion, and perhaps another one, I could not insist that we amend the agenda in order to proceed immediately with a discussion of this motion.

[*English*]

The Vice-Chair (Mr. David Tilson): The chair is here really at the pleasure of the committee, and our guests have been asked to come here. The meeting goes from 9 until 11 o'clock. Normally what happens in these situations is that, if there's time at the end of the session, we proceed to other business.

Your proposed notice of motion is the second piece of business. If the committee wishes to make a declaration that this portion of the meeting on identity theft is to end at 10:30, then so be it. I'm not going to make that ruling. I would require direction from the committee. If the committee wants to do that, they're going to have to tell me. Otherwise, we will proceed with this delegation until whenever it ends, which could be 10:30 or it could be 11 o'clock.

It's really up to the committee, Madam Lavallée.

● (0935)

Mr. Sukh Dhaliwal (Newton—North Delta, Lib.): How would you like to handle this then? Would you like some direction?

The Vice-Chair (Mr. David Tilson): I'd like a vote. I'd like some sort of direction.

[*Translation*]

Mrs. Carole Lavallée: The solution would be to put the question to a vote. I think we can vote on my request immediately. I don't know whether you call that a motion in your jargon, but I ask that we set aside 30 minutes at the end of this meeting, that is to say from 10:30 to 11:00 p.m., to discuss the motion on the agenda.

Do you want us to vote with a show of hands? Perhaps we could simply request unanimous consent.

[*English*]

The Vice-Chair (Mr. David Tilson): I'll take that as a motion.

Mr. Wallace.

Mr. Mike Wallace (Burlington, CPC): Thank you, Mr. Chair.

I'll support that, as long as the word "approximately"—If somebody is in the middle of a speech or in the middle of a question at 10:30, I don't think we have to end right at 10:30, but as long as we finish up around that time and give some time to Madam Lavallée's request, I think we can handle that.

The Vice-Chair (Mr. David Tilson): There seems to be a general consensus.

Commissioner, your presentation, I guess, will end at 10:30, but thank you.

Madame Lavallée, you still have a bit of time left.

[*Translation*]

Mrs. Carole Lavallée: Thank you very much, Mr. Chairman.

Indeed, I have a lot of questions to ask, and, since I have stolen my own time, in a way, I will speak quickly, to the interpreters' great despair.

You said in your presentation that part of the problem of identity theft, and of the solution to that problem, falls under provincial jurisdiction. I'm particularly interested in that. Can you sort that out? What concerns the provinces and what concerns the federal government?

Ms. Jennifer Stoddart: With your permission, Mr. Chairman, I'll ask our lawyer to explain which part of the problem of identity theft might fall under provincial jurisdiction.

Mrs. Lisa Campbell: Good morning.

It is up to the provinces to enforce the act, the Criminal Code. So if an offence is committed under the Criminal Code, it is up to the provinces to decide whether or not they will prosecute someone for identity theft, fraud, or petty theft. The remarks I made earlier on the applications of the Criminal Code concerned that.

In addition, if personal information is like property, it's the same situation. Normally, property is a provincial jurisdiction, so it is up to the provinces to decide what they want to do.

That is why the Commissioner said that it was really a national, even international program that concerns the provinces, the federal government and our international partners.

Mrs. Carole Lavallée: Indeed, Ms. Campbell, earlier you said that one of the problems was that identity theft was not recognized as such in the Criminal Code. Do you believe that including it in the Criminal Code would be a solution?

Mrs. Lisa Campbell: I agree with the Commissioner, that is to say that the sections of the Criminal Code are reserved for the most extreme cases. First, it would be important to educate the public on the value of their personal information. Then there are regulations. Our office is already doing a lot of things to protect personal information. There are a lot of civil measures. That's probably where you will find the greatest force, the most opportunities for making changes. If someone isn't responsible for the personal information in his or her possession and that has tax consequences, that organization or that person may pay more attention in future. In the Criminal Code, the criminal measures are really for the most extreme cases.

That said, we think that the current sections are really obsolete and do not apply to a situation in which someone collects personal information for criminal purposes. Yes, there are deficiencies.

Mrs. Carole Lavallée: When you say that the present measures are obsolete, do you mean that they are old, that they no longer correspond to the kinds of thefts that are committed today?

Mrs. Lisa Campbell: Yes, they are old. The sections dealing with fraud and theft concern property, that is to say your money, your house, your car. Personal information as such doesn't have a recognized value.

● (0940)

Mrs. Carole Lavallée: If personal information doesn't have any value, are there nevertheless any prosecutions?

Mrs. Lisa Campbell: Yes, there are prosecutions, but only at the time of use. So, if someone, for example, makes a list of the personal information of all the members of the committee, we can do nothing. If he doesn't use that information, we can do nothing.

Mrs. Carole Lavallée: He can do what he wants if he doesn't use it or if we can't prove that he uses it.

Mrs. Lisa Campbell: That's it.

Mrs. Carole Lavallée: You also said a little earlier that this was a provincial, federal and international problem. Can you explain to me why it's an international problem?

Mrs. Lisa Campbell: When these are people from the organized crime community—my colleagues who have worked at the RCMP could talk about this at greater length—it's really an international problem, that is to say that the information is gathered in Canada, but it can be used elsewhere, for immigration purposes or other criminal purposes.

Mrs. Carole Lavallée: You also said that we can prosecute the users of this information, but not those who collect it without using it. Does that mean that a young person who works at a convenience store, for example, or who copies credit cards or bank cards at the request of a person involved in organized crime who pays him $150 for each copy couldn't be prosecuted?

Mrs. Lisa Campbell: Precisely.

Mrs. Carole Lavallée: Are you telling me that it's an open bar for all the people who work at a convenience store and who copy credit cards?

Mrs. Lisa Campbell: Unless you have a direct witness or direct evidence that organized crime is involved, that the young people are working together, which is usually very hard to prove.

[*English*]

The Vice-Chair (Mr. David Tilson): We have to move on, Madame Lavallée. I'm sorry.

Mr. Martin.

Mr. Pat Martin (Winnipeg Centre, NDP): Thank you, Chair.

I'm also interested in the idea. I believe the recommendation of the finance committee was to urge the Minister of Justice to include identity theft as a specific criminal offence.

It has always struck me as odd that it's a specific criminal offence to steal a cow in this country, but it's not a specific offence to steal a car or an identity. The argument is that if you listed everything there would be a huge volume of all the things that it's against the law to steal.

I sense there is interest in listing identify theft because it gives a judge more latitude in sentencing. Otherwise, how do you quantify how serious the identity theft is if it's not identified? If fact, when there's no actual injury it's still a crime to steal someone's identity, even if it never does result in financial loss to them.

I understand your point, but do you not agree that if it were included in the Criminal Code it would make it easier to enforce and would send the message to the community at large that we take this very seriously?

Ms. Jennifer Stoddart: Absolutely. In the time I've been Privacy Commissioner I have repeatedly inquired about the possibility of amending the Criminal Code. I gather there's some work being done by the Department of Justice, but we have not yet seen it finalized. I hope that Justice will move on this.

Your colleague the honourable Mr. Rajotte of Edmonton Southwest introduced a private member's bill to amend the Criminal Code to cover identity theft. This has now passed second reading and has been sent back to the House. I have supported it, and people from my office have tried to give Mr. Rajotte any advice he has needed.

This is an urgent problem and we see a lamentable slowness in responding to it.

Mr. Pat Martin: You mentioned that the U.K. commissioner's report is shocking. Can you give us a brief example of some of the things that pop out of that report?

● (0945)

Ms. Jennifer Stoddart: Yes. In the U.K. it seems there is a multi-million-pound industry in illicitly obtaining personal information—I think the two main actors are the media and lawyers—to either aid their clients' side of affairs or expose public people in compromising situations.

I wonder if Carman Baggaley has read about this more recently than I have.

Carman, are there any other highlights?

Mr. Carman Baggaley (Senior Strategic Policy Analyst, Office of the Privacy Commissioner of Canada): As the commissioner suggested, I think partly it's fed by the media in the U.K., but there are many examples of people in either telephone companies or financial institutions being paid to disclose information that is then sent in to the media to highlight the social life or the private life of celebrities, and it's a very lucrative trade. There are companies for which this seems to be the main line of business—obtaining this information—which then feeds into various uses.

Mr. Pat Martin: I see.

The last thing I would raise is that the numbers you cited at the start of your presentation seem very low to me, although you do make the point that it's difficult to actually measure the depth and breadth of the problem. But 7,500 identity theft victims reporting $16 million in losses seem like a mere fraction of what's probably going on out there. Would you agree with that?

We were using an American figure of 30 million incidents per year and extrapolating 10% of that for Canada's population. Would that be reasonable?

Ms. Jennifer Stoddart: Yes, it's possible that it's much larger.

Could I ask the director general of investigations, who has worked in this area with the RCMP, to give you his opinion of what's really happening out there?

Mr. Wayne Watson (Director General, Investigation and Inquiries Branch, Office of the Privacy Commissioner of Canada): You're right; it is much larger, and the problem we're having in being able to get proper statistics is the fact, as Lisa said, that there's no law in Canada against identity theft. So it's very difficult, because identity theft being used for approximately 12 to 40 different offences renders it difficult to put together some statistics. If they're used for forgery, is it because of identity theft or not? That's why it's difficult.

However, going back to what you're saying about the United States, I think in February the data clearing house stated that there were 104 million records. The total number of records that were compromised in the U.S. between January 2005 and February 2007 was 104 million. So that will give you an idea. It was 586 publicized breaches, and we have had some breaches here in Canada. Obviously we've all heard it in the news. Our offices, I think, have been notified of close to 100 cases in the last four or five years, and every one has the potential for identity theft.

Mr. Pat Martin: Thank you.

The Vice-Chair (Mr. David Tilson): Thank you, Mr. Martin.

Mr. Van Kesteren.

Mr. Dave Van Kesteren (Chatham-Kent—Essex, CPC): Thank you, Mr. Chair.

Thank you, Madam Commissioner, for coming. Thank you for this great presentation. It's a serious problem we all know about. We all want to do something about it.

I want to address Bill C-299, a bill which I am familiar with. I'm going to speak on it, as a matter of fact, tonight, and I am the seconder of that bill.

There were some concerns, the concerns being that within the bill's writing, as it was originally drafted, Bill C-299 would have created offences that criminalized the very act of obtaining personal information by deception. The thought behind that was that legitimate circumstances for deception were used. They were talking about police possibly trapping criminals, or possibly even within a family. There are times when lying takes place and they didn't want to criminalize that. On the broader act, I guess the problem that cropped up was something that nobody really anticipated, and it underlines just how difficult legislation like this is.

Should we move forward and make recommendation for a broader act? Can you tell us of other areas possibly you see in the distance that could really create some problems, as what happened with Bill C-299?

● (0950)

Ms. Jennifer Stoddart: Can I ask Lisa Campbell to speak to that? Yes, there are issues of Criminal Code drafting and the issue of intent, particularly.

Mrs. Lisa Campbell: Thanks very much. You raise a good point.

There are two things we would point out with this bill and with any legislation that you put in the Criminal Code. First, you need to prove criminal *mens rea* with every criminal offence, which is to say criminal intent. That's an essential element of every offence.

Second, there is prosecutorial discretion. There are many offences in the Criminal Code—I think Mr. Martin mentioned one of them—in which crown prosecutors have discretion whether or not to lay a charge and they work with the police to do that. The issues you've raised are why we're recommending a range of measures: public education; some regulations, which our office is already involved in enforcing with PIPEDA and the Privacy Act, and higher standards for organizations; and then civil remedies, which are probably what you would use the most, reserving Criminal Code offences as a necessary but probably rarer last resort.

Does that respond to your question?

Mr. Dave Van Kesteren: Yes. Bill C-299 is a study on counterfeit and piracy. I think I can speak for the member who presented the bill, as he is the chairman of our industry committee, and we are studying a number of concerns that interconnect somewhat. I think even in our discussion this morning, one of the things that become obvious is that this isn't just a Canadian problem; this is a worldwide problem.

My question would be, are we at the stage where we should possibly be looking at international laws and—this might sound a little extreme—possibly even an international court to deal with some of these issues? Because it's not just happening here; it seems to spread right across this globe.

Ms. Jennifer Stoddart: Yes, you're absolutely right. Mr. Watson can talk to us about some of his experiences in cross-border fraud. This is one of the reasons I'm active in the OECD on cross-border enforcement of personal information protection rules. I don't think we need to think of going to an international court yet, but if we have rules that are recognized in other jurisdictions that have similar legislation to ours and we can probably help each other through either foreign courts or our own, I think that would go a long way.

Can I ask Mr. Watson?

Mr. Wayne Watson: The problem is definitely international in scope. The problem we have right now is that I think we're the only G8 country that does not have a law against identity theft. If we're going to have any credibility in the world, if we are going to be a world leader to try to tackle this problem, we're going to have to have a law to start with.

I think a lot of ID theft is perpetrated by organized crime, and it goes around the planet in seconds sometimes. We need cooperation so law enforcement or any regulatory organization can tackle it. We need to have the necessary legislation to be able to work cross-border. Perhaps we could do the same thing as we have with money laundering. I think the way we're working at it is a success across the planet, and I think identity theft is another issue we should look at it in the same manner as money laundering.

Mr. Dave Van Kesteren: I want to talk about national ID cards and biometric ID and RFID, something that I pulled up on your web page.

Madam Commissioner, you and I have had some discussion about how the world is moving so rapidly. Things we would never have thought about ten, let alone five, years ago are approaching us so quickly. I wonder if you want to tell us about these new security devices and these tracking devices and what kinds of privacy problems they will create.

Ms. Jennifer Stoddart: Can I refer that to our technological specialist, Mr. Chairman?

Mr. Steve Johnston (Senior Security and Technology Advisor, Office of the Privacy Commissioner of Canada): Thank you.

The major problem that seems to crop up in any discussion of national identity cards is proving the identity initially. For example, when you go to get a passport you produce a birth certificate, a driver's licence, a health card, what we refer to as foundational documents. These can be forged, and unless you have some very high degree of confidence that the individual who is presenting these documents has proof of identity—

● (0955)

Mr. Dave Van Kesteren: I'm sorry to interrupt. What about RFID?

Mr. Steve Johnston: I'll get to that. Unless you have a very high degree of assurance that the individual presenting the credentials is entitled to do that, what you end up doing is issuing a very secure document obtained under false pretences.

In terms of RFID, there are efforts in several countries to embed these in various forms of identity documents—driver's licences, health cards, etc., the notion being that it will make the particular transaction that the card is designed for quicker, more efficient. For example, you don't need to swipe the passport. You just need to wave it by the reader. The problem with that is that until fairly recently that communication was not protected in any way. So anybody who had access to the radio frequency spectrum could read that information.

The Vice-Chair (Mr. David Tilson): We have to move on, I'm sorry. Maybe somebody else can ask another question to get into that, but I'm trying to follow the rules.

We'll go to Mr. Dhaliwal.

Mr. Sukh Dhaliwal: Thank you, Mr. Chair.

Madam Commissioner and your talented team, welcome. That was very well presented.

This is the type of stuff that will help us to make up our minds. Now it becomes a question of leadership. Who is going to provide the leadership to deal with this situation of identity theft? Mr. Van Kesteren mentioned the international courts, and Mr. Watson was mentioning the money laundering situation.

On that same theme, the Canada Revenue Agency continues to report that Canada is losing a lot of money through grey and black transactions. And they have been far ahead dealing with that situation internationally and tracking down that money. In your opinion, would they be better positioned to take a lead than the Department of Justice, or to coordinate with the Department of Justice?

Ms. Jennifer Stoddart: Is your question whether FINTRAC could coordinate with the Department of Justice?

Mr. Sukh Dhaliwal: Like with Canada Revenue Agency, right?

Ms. Jennifer Stoddart: First of all, I think it's up to the Government of Canada to decide how best it should deal with this. But I would say that it's a natural role for the Department of Justice. This is a law legitimacy issue. But there are many agencies, ranging from FINTRAC on one hand, to the RCMP, to the Competition Bureau, to Industry Canada, that doubtless have a wealth of knowledge about the different forms of circulation of information and information technology and so on.

I don't know if that answers your question.

Mr. Sukh Dhaliwal: Probably not.

To deal with this situation now, because there are hundreds of agencies involved, we have to have a clear department or clear leadership to deal with this situation. Who, in your opinion, would be the best person to deal with this?

Ms. Jennifer Stoddart: Well, I think this should be considered carefully. I don't know if it is. I would think that in order to consider it, the Department of Justice should look at this and ask what the structure is. Is it a permanent or a temporary structure? How do we set it up? How do we set it up within the Government of Canada, and then how do we cooperate with the provinces? The municipalities may have a role. The private sector has a huge role if you think of the banking and financial interests, plus internationally. There is also Industry Canada, which originated PIPEDA, so Industry Canada is another possible leader in this field.

Mr. Sukh Dhaliwal: Does the U.S. have a central agency that deals with this situation?

Ms. Jennifer Stoddart: The U.S. has the Federal Trade Commission, which enforces consumer protection laws. They don't have a national privacy act, and one of the things that hamper their fight against ID theft is that there are no national standards for personal information protection. But they do have a very efficient agency, the Federal Trade Commission, that has set up a clearing house for ID theft. I think it has been quite successful in gathering statistics and, to some extent, in educating the public and prosecuting, but not completely, which is why the President called for a special report on it.

● (1000)

Mr. Sukh Dhaliwal: In your opinion, should we have something like that? Would the clearing house in the U.S. that you mentioned help?

Ms. Jennifer Stoddart: Yes, I think that's one of the possibilities. And you don't have to have either a task force or a clearing house. Presumably one of the roles of the task force is to document all this. How does it happen? What are the problems from different perspectives? Who can bring remedies? It's not just a criminal law issue; it's also a civil law issue, it's an issue across Canada enforced by the provinces, and so on.

So I think you need some combination of a study group and somebody who's going to run a central depository of information and analyze the information in order to capture the trends and suggest the solutions.

The Vice-Chair (Mr. David Tilson): I have two questions before we proceed to Mr. Stanton.

First, what role can your commission play?

Ms. Jennifer Stoddart: I've tried to briefly indicate the role that we have. We've done a lot of ongoing education on personal information protection. We do investigation of cases relating to it. I mentioned the cases having to do with unsolicited credit cards arriving in the mail with your name on it. I think that practice has been virtually eliminated because of the problems it obviously posed to one's own personal information. We are concerned with convenience cheques. We have had quite a few discussions with the Canadian Bankers Association about convenience cheques, again arriving in your mailbox, where they can be stolen, in the wrong mailbox, and so on.

All the standards that we enforce through our complaints system —I say “enforce” because we enforce them on a consensus basis— have to do with the more secure storage and protection of personal information. That goes to inadequate shredding, inadequate disposal, updating lists, who has access to your personal information among companies or within the Canadian government.

The Vice-Chair (Mr. David Tilson): The second question is perhaps to Ms. Campbell, as to whether she has any jurisdictions that the Canadian government should look at to model either new sections of the Criminal Code or the tightening up of existing sections of the Criminal Code.

Mrs. Lisa Campbell: That's a good question. We probably should look to Commonwealth countries because of the similarities in our judicial systems. But it's a new problem internationally. I think what we're seeing here is its emergence as a criminal problem because of the value of personal information as a commodity.

There are not a lot of examples out there. It's a good idea to talk with our international counterparts to see what they're doing. Many are establishing task forces, as the U.S. is doing, and developing and considering criminal sanctions, civil sanctions. So it is a good idea to consult with them, to make sure that if we end up doing international agreements we're on the same page.

The Vice-Chair (Mr. David Tilson): Thank you.

Mr. Stanton.

Mr. Bruce Stanton (Simcoe North, CPC): Thank you, Mr. Chair.

Thank you to our panel, again, this morning.

I have a whole bunch of different questions. This is obviously the first testimony that we've heard on this topic, so it's a real eye-opener in some ways.

One of the things that I was quite intrigued with early on...and just as a point of background, when we decided to engage in this topic, we initially considered that we wouldn't be that interested in the criminal side of it so much. I see by your presentation here today that in fact it very much encompasses that, because one part of the toolbox is going to be the criminal side, if you will.

Actually, the chair jumped on a question that I wanted to spend a bit of time with as well, and maybe I'll build on that.

In terms of that toolbox, your office will be part of that. We've already spent some time on PIPEDA. I wonder if you could continue on along the same lines. I noticed that in your remarks you talked about some additional measures that could be taken in the Privacy Act. What other things do you see your office providing in terms of leadership and moving this forward?

Ms. Jennifer Stoddart: Thank you for that question.

I think making sure that the information rights of Canadians are up to date is clearly part of that general picture. That's why I'm happy this committee, as I understand, is thinking of moving to the issue of the reform of the Privacy Act, which is the basic law governing the relationship between Canadians and the federal government in terms of the personal information the government holds for them and on their behalf. I've pointed out several times that this is inadequate, so that's certainly one thing that can be done.

As you probably know, my office now has a more extensive audit program of federal government agencies to make sure they are holding personal information appropriately, that the databases are not likely to be hacked into, that there are appropriate safeguards in place to prevent employees, as unfortunately could happen from time to time, selling this information. We regularly investigate, it seems, laptops here or there that are stolen or forgotten. You can read our past annual reports. There's a history of that. I think there have been fewer recently, which is a good sign.

In terms of the federal government, I think our presence and our role helps to maintain a higher standard of information security and confidentiality within the federal government.

● (1005)

Mr. Bruce Stanton: I have one other brief question.

On the global picture, you had some references to the task force in which the U.S. is involved. Do you know of anything that's happening at an international level, for example at the UN? Because of digital technology, there's a real flattening there. These issues can crop up not just in North America but on the other side of the world.

Is there any coordination at the international level?

Ms. Jennifer Stoddart: I'll ask Steve Johnston if he can tell you about it, because he coordinates the technological issues. He follows that internationally for us. There's certainly a London action spam plan, but you're asking about international initiatives.

Mr. Steve Johnston: I'm not aware of anything dealing specifically with identity theft. I know there are efforts under way under the OECD to deal with cross-border enforcement of privacy law. That is going to be a huge issue, considering how easily personal information can be moved across borders. It involves harmonization of legislation, putting in place agreements between law enforcement agencies to enable mutual assistance, and so on.

The commissioner alluded to the London action plan, which is an international group dealing specifically with the spam problem. It consists of members of the OECD, the European Union, and other groups. Because spam is one mechanism used to deliver phishing attacks, Trojan horses used to collect personal information, etc., it will have an indirect benefit in solving the identity theft problem. It's just one piece of a large puzzle.

The Vice-Chair (Mr. David Tilson): Thank you.

Monsieur Vincent.

[*Translation*]

Mr. Robert Vincent (Shefford, BQ): Thank you, Mr. Chairman.

Welcome, Ms. Stoddart. You talked a little earlier, but I just understood that it was the responsibility of Industry Canada.

What was it? Industry Canada should conduct a study on the measures that we can adopt or not adopt. Is that it? Can you tell me a little more about that? I only understood that passage, because some segments were in French and others in English. What was the Industry Canada study about?

Ms. Jennifer Stoddart: It was in response to the question by your colleague Mr. Dhaliwal. Who could conduct such an initiative to coordinate the fight against identity theft? I talked about Justice Canada, but I'm also suggesting that you start a dialogue with Industry Canada representatives.

Industry Canada had the Personal Information Protection and Electronic Documents Act drafted. Industry Canada has a lot of expertise in the field. Industry Canada heads Canada's delegation to the OECD and to the group working on the implementation of transborder measures on the protection of personal information.

I don't know whether they're appearing before you, but they have a lot of expertise in this field.

● (1010)

Mr. Robert Vincent: That's a happy coincidence, because I'm a member of the Standing Committee on Industry, Science and Technology, and we're preparing the upcoming meetings today. I'll take care of that.

Let's talk about another sector. You also mentioned thefts of unshredded documents from containers. You were pleased that the idea of raising personal protection standards had been talked about in Edmonton. What should we amend in the act or what measures should be taken to prevent people from finding documents containing personal information in garbage cans or elsewhere? I don't want to talk about giving people a little more education or making them more aware of their responsibilities; those are passive measures. We can say that the speed limit on the highway is 100 km/hr and that, if you drive at 150 km/hr, there will be consequences. It's the same thing here. We're saying that documents containing personal information should be shredded, but, if we find them in the garbage can, what do we do? Do we rap the person who is at fault on the knuckles and tell him not to do it again? Is there a more aggressive measure that we can implement to make people aware that the confidentiality of personal information is important. To that end, what measures should be taken with regard to these businesses or these people who lose our personal documents.

Ms. Jennifer Stoddart: Various statutes on the protection of personal information apply to businesses. In addition, penalties can generally be imposed, in accordance with those statutes, if we show that harm has been caused. One of the current problems is that there is no statutory system of fines for having done something.

Mr. Robert Vincent: You talked about fines, didn't you?

Ms. Jennifer Stoddart: I'm telling you that, for example, the federal act does not provide for a system of fines. You have to prove damage has been caused. That's part of the problem of defining identity theft. Throwing away information without shredding it isn't, in itself, something for which you should be directly punished. If one of the federal or provincial commissioners heard about the incident, he would intervene in order to say that you absolutely have to change the way you do things, or else he will prosecute you, institute proceedings against you.

Mr. Robert Vincent: That's what I just said; it isn't just a little rap on the knuckles. We tell them to stop doing that, to stop throwing away papers because that can hurt someone somewhere. There aren't any tougher measures for these people to make them aware of the fact that this is important.

Would you recommend that there be a fine or something tougher that tells people that this information is invaluable, that they have to be careful with it and not throw it away? Would you recommend that approach?

Ms. Jennifer Stoddart: That's one of the options that a task force should consider. As I mentioned a number of times during our meeting this morning, we need a range of penalties, and not just resort to the Criminal Code. We have to prove intent, which is hard to do.

A system of fines, if you think of it, is a little like the way it is for the environment. For people to be aware, you have to tell them that, if they throw away something toxic, they will be liable to a fine. However, I don't know whether we've got to that point. You should consider that possibility.

[*English*]

The Vice-Chair (Mr. David Tilson): Thank you.

I'm sorry, we're way over, Monsieur Vincent.

Mr. Wallace.

Mr. Mike Wallace: Thank you, Mr. Chairman.

I have a couple of questions, and they sort of start at the beginning.

I was reading over what you provided—and what you provided us with today is excellent—and you do have information here on how to protect yourself. One of the points was to avoid collecting and using your SIN, your social insurance number. You know, we use it. Service Canada has an ad on the television trying to convince people to get their SIN numbers so that they can get a job. We also have a senior's card. It has come to my attention recently that the number we use on the senior's card is the SIN number. It gets sent through the mail, and so on and so forth, because it's the only number, I think, that the Government of Canada has to identify individuals.

I would like your comment on what the options are, other than using your SIN number for different things. From a privacy perspective, as commissioner, have you had a chance to look at that at all?

● (1015)

Ms. Jennifer Stoddart: Yes, that's one of the things we look at, perhaps not in detail.

Can I ask Carman Baggaley to speak to the issue of SIN numbers and the vulnerability that they can cause for Canadians?

Mr. Carman Baggaley: One of the points we made is that we need a much clearer idea of what the underlying problems and causes are for identity theft. One of the things we know is that there is a great deal of concern that the social insurance number can be used for identity theft. If we had more information about what's actually causing identity theft, then we'd have a much clearer idea of the extent to which problems with the SIN contribute to it. There have been concerns that there were more SIN numbers out there than there are live Canadians. We're told that's being fixed. But that's one of the many areas where we really need to know what the various factors are that are causing the problem. Then we can decide how we need to proceed in terms of the SIN. Do we need to restrict its use further, or in fact is it not as much of a problem as some people think?

In the online world, of course, there are alternatives to the SIN. That's what the whole secure channel is about, where randomly generated numbers are used to identify people.

Mr. Mike Wallace: I have another basic question on something that was brought to my attention by a constituent.

I know you talk in other documentation you have here about people phishing to get information about people, usually on the Internet, and what there is in terms of your name, birth date, and all those things that happen to be maybe on my Facebook, which somebody else looks after. One question came to me from a constituent, and I didn't have a good answer for them. They were unhappy that their phone number and address were in the phone book because that would be the beginning of somebody finding out who they were and where they lived, and then they could go through their garbage and they'd have a start.

Is there a law that exempts the use of that information in the publication of the phone book?

Ms. Jennifer Stoddart: No, I don't think there's any law that addresses that, but you can ask that your number be confidential. You can ask that your number be taken out of the directory.

Mr. Mike Wallace: You have to pay for that service, and that was one of their issues. Here they are, interested in trying to be as private as possible, and it's costing them money to do so. It had never been brought to my attention—since I don't mind being in the phone book—that this is people's information. It's not their SIN number or something you could go to the bank and use, but it would be a start.

No one has challenged this in the courts that you know of? Can anybody answer that question?

Ms. Jennifer Stoddart: Before I became the Privacy Commissioner, there was the Englander decision that went up to the Federal Court about how people could choose and how the telcos had to respect their right to be out of a public telephone directory at a minimal cost. That was about the issue of consent and so on.

You're getting to the issue of privacy versus the fact that we do live in communities and we need a certain amount of public information to live in the community. If we're all anonymous in this society, I think that poses other problems. You could also question my colleague Robert Marleau, the Information Commissioner, on that.

The Vice-Chair (Mr. David Tilson): Are there any questions from the opposition?

We'll have Mr. Van Kesteren and then Madam Lavallée.

● (1020)

Mr. Dave Van Kesteren: Thank you, Mr. Chair.

Mr. Johnston, I want to go back to RFID, just for the sake of the committee. I found this really intriguing.

I had one of the techno wizards working for me, and we had quite a conversation when he was briefing me on this. I want you to elaborate on some of the concerns that the Privacy Commission has. Maybe just tell us quickly what this radio frequency identification technology is. What's involved? Briefly tell us, and then tell us why you're concerned about some of this technology and where it might go.

Mr. Steve Johnston: Thank you. I was kind of hoping you'd come back to that question, because we didn't get to it the first time.

Radio frequency identification systems typically consist of these components: the tag itself, which may or may not have processing capability; the antenna, which is part of the tag; a reader that emanates radio frequency energy, which is used to power passive tags; and then the software that interprets the information that comes back from the tag to the reader, because usually all that the tag contains is what's known as the electronic product code. You then have to look up in a database what that code is associated to in terms of the product, when it was manufactured, what its pedigree is, etc.

The privacy concerns around RFID stem partly from the fact that it's very small. It can be embedded in virtually anything, and it can give up its code or any other information that's stored on the tag without the individuals being aware that it's actually being read.

The major concern is that even if you can't necessarily associate a particular tag to an identity—in other words, tag number 123456789 is associated to me—you can associate the tag with a person of interest. For instance, it has been rumoured—and I don't know how true the rumours are—that law enforcement agencies have been using surreptitious readers to identify tags that are on objects possessed by individuals. So we get to the point where items of clothing, for example, are tagged. What you end up with is a series of numbers that are associated with a particular individual, and if that particular individual is at anti-war rally or some other form of protest, that marks them as a person of interest. If at some point that individual goes to go through a border control point, for example, and those tags are read again, they've now made the association to a specific identity and can take the individual aside for secondary screening or whatever.

So the notion of the RFID tags as a proxy for an identity is an issue of concern for us.

Mr. Dave Van Kesteren: But it certainly opens up some exciting new prospects, and I guess I'm looking for that balance. There's some wonderful technology here that can really benefit mankind, and we don't want to stifle that. At the same time, we don't want it to be abused.

Have you found a little bit of a balance there? Are you looking at that?

Mr. Steve Johnston: The tipping point seems to come at the point where the tags come in contact with individuals. For example, supply chain optimization is great technology, and we're all for that simply because it makes things more efficient, more cost-effective, and so on. At the moment, that's where the bulk of RFID use is. We're tagging large items. We're tagging cases and pallets; we're not tagging individual objects.

The concern is that at some point the technology will become cheap enough and small enough that it will be embedded in everything. The way the electronic product code is constructed, every single object on the planet could have a unique identifier. So unlike the bar code, where every can of Coke has the same identifier, every can of Coke could have a unique identifier. If that becomes associated with an individual and then is used for invasive marketing or tracking, or something like that, that's where we have the concern. Up to that point, it doesn't seem to be much of an issue, either at our level or with other commissioners around the world.

● (1025)

The Vice-Chair (Mr. David Tilson): Thank you, sir.

Madam Lavallée.

[*Translation*]

Mrs. Carole Lavallée: Earlier you talked about the Commonwealth countries, but also about the countries that were particularly effective or that were forming task forces to see how to solve the problem. If I did an Internet search, what countries could serve as models?

Ms. Jennifer Stoddart: For your guidance, we've included the summary of the U.S. study. The Americans are trying to solve this problem, but they don't have laws with standards similar to those of Canada. Credit access conditions in the United States are much more relaxed than in Canada. The problem may be more serious there.

Internationally, we are virtually all dealing—I don't know whether there is one country—

Mrs. Carole Lavallée: We're all at the time stage.

Ms. Jennifer Stoddart: That's correct.

Mr. Watson, I don't know whether you are familiar with white collar crimes, which are a kind of fraud. Is there one country that can serve as a model?

Mr. Wayne Watson: Not really. The Americans, by the size of their population and under the legislation, are on the lookout for the latest investigation technologies and techniques. However, this is an international problem. We can control certain things here at home, but we can't do it elsewhere. We'll eventually have to find an international solution to solve the problem of identity theft. No country will be able to solve it. It's too big a problem.

Mrs. Carole Lavallée: All right.

Mr. Tilson, it is 10:28 a.m. So I'm going to stop there.

[*English*]

The Vice-Chair (Mr. David Tilson): You want to cut yourself off, Madam Lavallée?

Madam Stoddart, thank you very much, and to your colleagues, for appearing before us, and for the book, which we will refer to. We will be asking other witnesses to come to this committee and it may be that in the future we will ask you to return.

Thank you, to all of you, for coming and making your presentation to us.

We will recess for a couple of minutes to allow the commission to retire.

● _____ (Pause) _____

●

● (1030)

The Vice-Chair (Mr. David Tilson): We're going to reconvene, ladies and gentlemen. I would ask for some order in the room.

Madam Lavallée has requested to have the floor at 10:30.

[*Translation*]

Mrs. Carole Lavallée: Thank you very much, Mr. Chairman.

I started talking about this last week. You received a motion in both official languages. Recently, an internal report of the Department of International Affairs was the subject of a number of questions in the House and of a number of interviews.

[*English*]

The Vice-Chair (Mr. David Tilson): Madam Lavallée, to make this appropriate, perhaps you should actually make the motion. Please move the motion for the record and then we will proceed with debate.

[*Translation*]

Mrs. Carole Lavallée: I'm going to go about it in the order you wish, Mr. Chairman.

The motion that I introduced was as follows:

> That the Standing Committee on Access to Information, Privacy and Ethics urgently address the internal report by the Department of Foreign Affairs entitled *Afghanistan-2006: Good Governance, Democratic Development and Human Rights*, a report that the government claimed did not exist and took every step to prevent its release but was finally forced by the Information Commissioner to reconsider and then published the report but in a highly censored form.

That is the motion that I introduced. May I now present my arguments, Mr. Chairman?

[*English*]

The Vice-Chair (Mr. David Tilson): Do you have a point of order, Mr. Wallace?

Mr. Mike Wallace: On a point of order, Mr. Chairman, if I look at the bible around here, the House of Commons procedures book, on page 449 it says: "A motion should not contain any objectionable or irregular wording. It should not be argumentative or written in the style of a speech."

My suggestion to you, Mr. Chairman, is that this motion is out of order because it is against those rules. I would like you to rule on that.

The Vice-Chair (Mr. David Tilson): Mr. Dhaliwal.

Mr. Sukh Dhaliwal: Thank you, Mr. Chair.

In looking at this particular situation, *The Globe and Mail* received a report that was clear. The way I look at it is—

The Vice-Chair (Mr. David Tilson): We're talking on a point of order. Are you?

Mr. Sukh Dhaliwal: That's what it is. That's what I'm saying right now—a point of order, yes.

The Vice-Chair (Mr. David Tilson): Thank you, sir.

Mr. Sukh Dhaliwal: Look at it this way: when you compare, members of Parliament have had less access to this report than the media.

I think we should debate this and see how we can work together, on both sides of the floor, to make this workable. We have worked on this for many days, so we should at least get out of here with some consensus.

An hon. member: Are we debating the point of order?

The Vice-Chair (Mr. David Tilson): We're not in debate on the point of order. I think members are entitled to speak on the point of order if they have a point of order.

Monsieur Vincent.

[*Translation*]

Mr. Robert Vincent: First of all, if Mr. Wallace thinks that we are not on the right track, we still have the clerk. Then, if we think that the motion is admissible, we need only move on to the vote.

[*English*]

The Vice-Chair (Mr. David Tilson): No, Mr. Vincent, the clerk is here to advise the committee. Just to be clear, he doesn't make decisions.

Proceed.

[*Translation*]

Mr. Robert Vincent: Pardon me, I didn't mean that the clerk had to make such a decision, but he can tell you what the procedure is. I don't want him to make any decisions.

[*English*]

The Vice-Chair (Mr. David Tilson): No, he doesn't talk, sir. He advises the chair and the members of the committee. He doesn't make presentations.

[*Translation*]

Mr. Robert Vincent: Mr. Chairman, are you trying to play the fool with me? You understand very well what I mean. I simply mean to tell you that he is able to advise you. I don't want him to talk; that's clear and I understand. I want him to advise you, if Mr. Wallace does not agree, on the admissibility of the motion. Let us put the question to a vote. If we think Ms. Lavallée's motion is admissible, let us put it to a vote, and, if it is agreed to, then we will discuss it.

Mr. Wallace is interpreting the motion by the book, but he's making no reference to this. He's asking the clerk to tell you whether Ms. Lavallée's motion is admissible based on her remarks. Once Mr. Wallace and the clerk have given you their interpretation, we can vote. We're not going to conduct a debate on the debate. We will wind up voting on these two things, and once that's done, we can debate the merits of the question.

● (1035)

Mrs. Carole Lavallée: It's my turn, Mr. Chairman. I asked to speak.

[*English*]

The Vice-Chair (Mr. David Tilson): Madame Lavallée, on the point of order.

[*Translation*]

Mrs. Carole Lavallée: I don't want to argue the admissibility of my motion. I'm very surprised at the remarks of my colleague Mr. Wallace. I'm sure my motion is perfectly admissible because it doesn't contain any argument. It's simply a description of the events that have occurred.

Mr. Chairman, before the meeting, I spoke to my colleague Mr. Wallace, and we agreed—I don't know whether he still agrees—that he would introduce another motion. So I would be prepared to withdraw my motion so that he can introduce his, and we'll vote. Then let's see what happens. I agree to withdraw my motion, not because it isn't admissible, but because there is another one that would achieve more of a consensus and that would ultimately have the same purpose, that is to say to receive witnesses and to ask them what happened with regard to the administration of the Access to Information Act and this internal report. If his motion, even worded differently, has the same objective, I'll be in favour of it.

[*English*]

The Vice-Chair (Mr. David Tilson): You know, the chair is here to make rulings. You can't make a conditional withdrawal. You either withdraw it or you don't.

Do I understand, Madame Lavallée, that you are withdrawing your motion?

[*Translation*]

Mrs. Carole Lavallée: I'm going to withdraw it; there's no problem. My idea wasn't to make it conditional, but to explain the situation and the reason why I was withdrawing it.

[*English*]

The Vice-Chair (Mr. David Tilson): Thank you very much. You are formally withdrawing your motion,*oui*?

You know, we either have to get on with this or—We're going to recess for a couple of minutes.

● _____ (Pause) _____ ●

The Vice-Chair (Mr. David Tilson): We're going to reconvene the meeting.

Madam Lavallée, am I to understand you're withdrawing your motion?

[*Translation*]

Mrs. Carole Lavallée: Yes, Mr. Chairman.

[*English*]

The Vice-Chair (Mr. David Tilson): Thank you very much.

Mr. Wallace has the floor.

Mr. Mike Wallace: Thank you, Mr. Chair.

I will read a motion that I have. It's not translated. I wrote it last night. I'm just giving the committee notice. I'll read it, but I'll bring it officially to the next meeting, if that's fair:

> That the Standing Committee on Access to Information, Privacy and Ethics address the internal report by the Department of Foreign Affairs entitled *Afghanistan 2006: Good Governance, Democratic Development and Human Rights*. This review is to occur after the Information Commissioner completes his rulings on any and all ATI requests his commission has received regarding this document.

● (1040)

Mrs. Carole Lavallée: Can you just read the last sentence?

Mr. Mike Wallace: Sure. It is: "This review is to occur after the Information Commissioner completes his rulings on any and all ATI requests"—access to information requests—"his commission has received regarding this document."

If I can speak to my motion—

The Vice-Chair (Mr. David Tilson): No, you can't speak to it. This is a notice of motion.

Mr. Mike Wallace: I'm just giving notice that it will be in writing in English and in French, hopefully for the next meeting. I know I have 24 hours. I am going to try to get it by the next meeting. If not, it will be on Tuesday for Thursday.

The Vice-Chair (Mr. David Tilson): Okay, and you are going to give this notice of motion to the clerk, who will arrange for translation.

Mr. Mike Wallace: That's right. I need to do it, but not in my scratchy handwriting.

The Vice-Chair (Mr. David Tilson): Thank you very much.

Mr. Vincent.

[*Translation*]

Mr. Robert Vincent: I hope Mr. Wallace will check his motion against the article he has distributed to us. It shouldn't be a speech. However, the way in which he spoke was reminiscent of a speech. I'd like it to be more condensed.

[*English*]

The Vice-Chair (Mr. David Tilson): Stop. The notice of motion has been made.

If there is no further business, we will adjourn until Thursday morning at 9 o'clock. Is there further business?

[*Translation*]

Mrs. Carole Lavallée: Mr. Chairman, the committee has received a motion at the table a number of times. In another committee, we received a motion like this one, and the entire committee agreed to accept it and to vote on it when it was introduced. I remember that very clearly. Mr. Regan, you were on the Human Resources Committee when we debated the anti-strike breaking bill. That's what we did. A motion was introduced, and we accepted it.

The motion is announced. I'd like us to debate it and to vote on it immediately.

[*English*]

The Vice-Chair (Mr. David Tilson): Madame Lavallée, you're making a request that it be debated now—is that what you're saying?—in spite of the fact that it hasn't been translated.

[*Translation*]

Mrs. Carole Lavallée: Of course. I've received the translation. I'd like to debate it now.

[*English*]

The Vice-Chair (Mr. David Tilson): The chair will take the position that if there is unanimous consent, you will have your request.

Is there unanimous consent?

Mr. Mike Wallace: No.

The Vice-Chair (Mr. David Tilson): There doesn't appear to be unanimous consent, Madam Lavallée.

Mr. Regan, do you have a point of order?

Hon. Geoff Regan (Halifax West, Lib.): Mr. Chair, I just want to note that this must be a first, for a member to deny unanimous consent for his own motion to be heard and discussed in a committee.

The Vice-Chair (Mr. David Tilson): Thank you, Mr. Regan.

Thank you very much. The committee is adjourned until Thursday morning at 9 o'clock.

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

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

Also available on the Parliament of Canada Web Site at the following address:
Aussi disponible sur le site Web du Parlement du Canada à l'adresse suivante :
http://www.parl.gc.ca
