HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Human Resources, Skills and Social Development and the Status of Persons with Disabilities

HUMA • NUMBER 067 • 1st SESSION • 41st PARLIAMENT

EVIDENCE

Thursday, February 14, 2013

Chair

Mr. Ed Komarnicki

Standing Committee on Human Resources, Skills and Social Development and the Status of Persons with Disabilities

Thursday, February 14, 2013

● (1105)

[*English*]

The Chair (Mr. Ed Komarnicki (Souris—Moose Mountain, CPC)): I call the meeting to order.

Good morning, everyone. We'll get ready to get started.

I have some general comments I want to make, and then we'll begin by hearing from the deputy minister with respect to the issues before us.

You will have your earpieces, and there will be translation as we go. Of course we all know that ensuring the security of our personal data is a grave matter for all Canadians, particularly those who are affected.

It's the motion of Mr. Cleary, as amended by other members, that brings us before the committee. Essentially, I just want to say what the motion relates to.

It talks about a privacy breach, which of course is a matter of grave concern to all Canadians, particularly those involved. We are here to hear you explain how the privacy breach occurred, to explain what actions have been taken to ensure the security of personal data throughout the department, and what long-term solutions for affected Canadians will be put in place to protect their identity.

Those are the key and central issues, so you can expect questions in that area. After you've presented, each of the parties will be asking questions with regard to those three areas.

Of course, I'm not unmindful of the fact that the privacy commissioner is investigating this issue. The matter has been turned over to the RCMP, and there is a potential for class actions. There may be some in place as we speak. Those are also matters that I take into account.

My plan has been to proceed with questions and answers for each party at seven minutes as opposed to five minutes. I would ask the members to generally respect the time so that hopefully we can do two rounds of questioning. I know we have some committee business at the end, but I would hope to go through the two rounds of questioning fully if we could. If we run out of time, I would ask this committee that we defer that portion, but if we finish early then we can deal with it.

Those are my opening remarks.

With that, Mr. Shugart, we will let you go ahead and make your presentation.

Mr. Ian Shugart (Deputy Minister, Department of Human Resources and Skills Development): Thank you, Chair.

Members of the committee, I'm Ian Shugart, the deputy minister of HRSDC. With me are the associate deputy minister, Ron Parker, the ADM of the learning branch; Al Sutherland, the head of our legal services, here to discuss issues of the statutes that govern our work; and the chief information officer of the department, Charles Nixon.

I just want to say that given the seriousness of these events and the issue before the committee this morning and before the department over the last several weeks, I had asked Mr. Parker, as the associate deputy minister, to take personal charge of the response, the follow-up, and the oversight of all of these matters. For many days over the last couple of months this has been virtually a full-time preoccupation for our associate deputy minister.

Chair and members of the committee, as the chair has said, we're here before you in regard to two security incidents in the department involving missing electronic storage devices containing personal information.

As my minister has said, and I repeat for the management of the department, the incidents are unacceptable. Sensitive personal information was stored on unencrypted portable storage devices and not properly secured. This should not have occurred.

The minister has also announced the measures we are taking to prevent these types of incidents from reoccurring.

On behalf of Human Resources and Skills Development Canada, I say to the committee that I apologize for the incidents.

[*Translation*]

I wish today to take this opportunity to offer to the committee a detailed account of what happened in the two cases, describe the actions we took in reaction to them, and the measures we have since put in place to mitigate impacts and prevent such incidents from happening again.

[*English*]

Let me begin with a chronology regarding each event. In both cases the activities were related to confirming the incidents, investigating the incidents, strengthening practices, and informing Canadians.

First, let me address the missing hard drive. On November 5, 2012, an HRSDC employee at national headquarters in Gatineau discovered that an external hard drive was missing and reported it to their manager, who was the only other person who knew the exact location of the device. The manager confirmed that they had not removed the hard drive. Other employees on the floor were then asked if they had seen or borrowed a hard drive. They had not.

The external hard drive was in a secure-access building, in a secure-access area, and was stored in a cabinet with a lock.

The team undertook multiple efforts over many days to search for the missing hard drive, including speaking to all members of the team and a number of searches of the employee's office, the employee's floor, and other floors in the building.

The missing hard drive was brought to the attention of the director on November 22, who then asked all managers and employees within the division to undertake additional searches for the hard drive. Again, efforts were focused on the recovery of this missing asset.

● (1110)

[*Translation*]

Former employees, and one former manager, from the same group as the employees were also questioned. Commissionaires and the local area network technician were also contacted and asked if a hard drive had been turned in, or picked up by someone. No device had turned up.

On November 26, the Director General was advised that the missing hard drive was the one used to create a backup of files from a network drive as part of a process to migrate files from one area of the server to another. Some personal information on clients and employees was stored on the network drive, and as a result, senior program management was advised immediately of the missing drive.

[*English*]

Search efforts by branch employees continued, and the departmental security officer was advised of the missing drive on November 28. As well, corporate security then began a number of activities to locate the missing drive, including detailed sweeps of the physical premises and interviews with current and former employees in the area from which the hard drive had gone missing. There was no evidence of malfeasance, and it was considered most likely that the hard drive was somewhere on the premises of the building.

At this time senior management requested that an analysis be undertaken of all the files located on the hard drive in order to determine what information had been lost. As a result of the analysis, completed on December 6, it was discovered that the external hard drive contained personal information on approximately 583,000 Canada student loans borrowers, including student names, dates of birth, social insurance numbers, telephone numbers, addresses, and Canada Student Loans balances. It also contained the personal contact information of 250 departmental employees. It was not password-protected or encrypted.

Extensive search efforts at the building where the hard drive was stored continued from December 8 to December 14, including additional comprehensive sweeps of the building's ground floor by the regional security office and the analysis of all of the Learning Branch's existing hard drives' contents. These efforts failed to recover the hard drive, and the department first informed the Office of the Privacy Commissioner on December 14 that an external hard drive containing personal information was missing.

From mid-December to the end of December there were further management interviews with employees and building management, and other similar hard drives were collected for analysis.

[*Translation*]

In the first week of January, a formal internal investigation was launched. Simultaneously, corrective measures were developed and Canadians were informed of the loss of the hard drive on January 11.

At this time, there is still no evidence of malfeasance or an indication that the personal information has been accessed or used for any fraudulent purpose.

In a separate and unrelated incident, a USB key with personal information also went missing.

On November 14, 2012, personal information was put on the USB key and given to an employee working on a secure floor in HRSDC.

● (1115)

[*English*]

The USB key was used on November 15, but on November 16 the employee could not locate the USB key and informed management. The same day departmental security officials were notified that the USB key could not be located. Extensive searches of the employee's office and the affected floor were undertaken by departmental security officers and by commissionaires from November 16 . The employee searched their home, and the taxi driver with whom the employee travelled home on November 15 was contacted and the taxi was checked. A team of employees also searched all files, filing cabinets, washrooms, furniture, and offices on the affected floor. Cleaners working on the floor were interviewed.

The USB key contained information on 5,045 individuals and was not password-protected or encrypted. The device contained the following type of information for each individual: social insurance number; surname; generic medical conditions by way of codes from the International Classification of Diseases; birth date; other payers, such as Workers Compensation; level of education; occupation; and Service Canada processing centre.

The department first informed the Office of the Privacy Commissioner on November 22 that a USB key containing personal information could not be located and that search efforts were under way.

[*Translation*]

Searches have continued since the incident, and another major effort was made on December 7 when an official, along with a team of employees, conducted yet another extensive search of the employee's office.

Notification letters were mailed to 5,000 affected individuals or their guardians on December 19.

I now want to highlight all of the actions we are taking as a result of these two incidents, and the measures we put in place to prevent similar incidents from happening again.

[*English*]

The department has strengthened its policies for the security and storage of personal information. Our actions focus in the areas of information hardware, information software, and our culture regarding the handling of personal information.

In regard to hardware, we have newer, stricter protocols. Portable hard drives are no longer permitted. Unapproved USB keys are not to be connected to the network.

In addition, there have been risk assessments of all portable security devices used in the department's work environment to ensure that appropriate safeguards are in place. These assessments will continue on a regular, ongoing basis.

With respect to software, we will be implementing new data loss prevention technology, which can be configured to control or prevent the transfer of sensitive information, and in regard to our culture of handling information, we are reinforcing the critical importance of the proper handling of sensitive personal information through annual mandatory training to be provided to all employees.

We are increasing awareness, and communication events and disciplinary measures will be implemented for staff, up to and including termination, should the strict codes of privacy and security not be followed. We have also taken actions to mitigate the impact on the Canadians affected.

[*Translation*]

We have alerted affected clients so that they can take the necessary steps to protect their personal information. This has been done through public announcements, by providing special information on dedicated web pages, by sending out letters to affected individuals and by the establishment of dedicated 1-800 toll-free information lines to respond to questions regarding both the missing USB key incident and the missing hard drive incident.

● (1120)

[*English*]

The affected social insurance number records have been annotated in the social insurance register to indicate that the social insurance number was involved in an incident and to ensure that any requests for changes or modifications undergo an enhanced authentication process. The department will also notify individuals for whom we have current contact information if the department notes any suspicious activity with respect to the client's social insurance number record. As a further caution, the department has purchased a customized package from Equifax Canada, which is a unique solution tailored specifically to this incident and is available to anyone who may have been affected. This credit protection is a reliable and appropriate strategy that will assist in preventing misuse of personal and credit information.

[*Translation*]

Through its agreement with Equifax, the department is able to offer, free of charge, its customized package to affected individuals who provide their consent to receive this service.

The notation will stay on credit files for a period of six years unless affected individuals choose to have it removed. The notation will alert credit grantors that data may have been compromised, and lenders will then take additional steps to verify the person's identity before granting credit or opening or using accounts.

[*English*]

Mr. Chair, the protection and security of personal information is a cornerstone of the department's mission. We are confident that we have taken the right steps in this situation, and we are making sure that they are followed to safeguard the personal information entrusted to us.

Thank you.

The Chair: Thank you for that presentation.

There is just one question that I have. You indicate the hard drive was stored in a cabinet with a lock and that only two people had access to that cabinet. Is that correct?

Mr. Ian Shugart: Yes, we confirm that.

The Chair: Okay.

I'll open the round of questions. We'll start with Ms. Borg.

Go ahead.

[*Translation*]

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

We are all concerned that half a million Canadians have lost their information. When we really do the math, we can see how huge the loss is.

[*English*]

For me this situation really demonstrates another example of the government's complete lack of respect for our personal information. We've seen a failure to update basic privacy laws that are supposed to be updated, and in the Privacy Commissioner's report to Parliament last year, she indicated that there has been over a 300% rise in privacy breaches. That is obviously the total for all the ministerial departments. Last year, in her 2011-2012 report, she reported 80 data breaches within government departments, which is a record high. Looking at this, I really see a systematic problem.

Now, I was wondering if you can answer me this: how many of those 80 reported data breaches were from HRSDC?

Mr. Ian Shugart: I believe—subject to your confirmation, Ron—it's 19, which is down a small, but to us important, two from the previous year.

Ms. Charmaine Borg: I personally consider 19 data breaches as being quite a high number in a year.

Mr. Ian Shugart: We regard that as something to be brought to zero and maintained at zero if at all possible.

Ms. Charmaine Borg: I'm very happy to hear that.

The Privacy Act actually doesn't make it mandatory for departments to report breaches to the Privacy Commissioner. You're saying that 19 breaches were reported. How many weren't reported?

Mr. Ian Shugart: We do have effectively a threshold that takes into account the nature and the seriousness of a breach, as well as the ability to contain a breach of any kind very quickly. There are, from time to time, incidents of that nature, and if we become aware of an incident, we move very quickly to contain it, but the threshold for informing the Privacy Commissioner is not a high threshold. We are frequently in touch with the Privacy Commissioner.

With respect to our practices, we take advice from the Privacy Commissioner. In this situation, we have, throughout the circumstance, been in touch with the Office of the Privacy Commissioner and taking advice, whether formally given under their terms of reference or counsel or practical direction. If an incident occurs and it is of a small scale and readily containable, we may not in that case inform the Privacy Commissioner.

● (1125)

Ms. Charmaine Borg: Are you saying that there are data breaches that have happened that have not been reported? Do you have a record of this? Can this be made public to the committee?

The Chair: Ms. Borg, if I might, I know you're building to where you're going, but this committee is looking at three things: how did the breach of privacy occur, what steps were taken as a result of that, and what future course of action will be taken with respect to a long-term solution for those that were particularly affected.

I know you're talking about things that may have happened in the past. Although they may have some relevancy in the general sense, specifically this incident is to be dealt with on its own. How it occurred, what steps have been taken as a result of that, and what will be done for those affected are the areas that we're dealing with.

I've given you quite a bit of latitude, but I'm asking you to bring it closer to the point of reference. If you don't do that, I'll rule it out of order.

Ms. Charmaine Borg: Thank you for that clarification, Mr. Chair, but I do think Canadians are quite preoccupied by the number of breaches that are happening within the government.

The Chair: It's this specific one.

Ms. Charmaine Borg: I understand. Thank you.

The Privacy Commissioner has begged, pretty much, the government to act and include mandatory breach requirements, data breach requirements, to government departments. Seeing as this is a data breach that happened, would you recommend, based on what happened here, that all departments be required to notify the Privacy Commissioner of data breaches?

The Chair: If you feel you want to, you can answer that, but it's not your responsibility in terms of what government might do for policy with respect to other departments. You're responsible for what happened administratively in this case. What may happen with respect to government policy and what the government might want to do or should do with respect to other departments is not part of this hearing.

Ms. Charmaine Borg: But they went through a data breach. They went through something, and they can.... I think we're all interested in fixing the systemic problems here.

The Chair: They can deal with it, yes, but I don't want to get caught up in what government policy should be or what other departments should do. We're here with this department on this specific breach, and that's what I want the questions to go to. Anything outside of that I will rule out of order.

Ms. Chris Charlton (Hamilton Mountain, NDP): With respect, Chair, I understand what the parameters are of the task before us here today, but what we are tasked to do is to look at the systems that are in place to protect the privacy of Canadians' personal information. It is appropriate to ask what those are in the Canadian government. That's what my colleague is asking. I think you have to give her that latitude.

The Chair: I'm not going to debate that any further. I'm ruling any questions that go outside of what we're talking about here, questions about other departments, as out of order.

You can answer if you wish, in a general way, but specifically refer to your department.

Mr. Ian Shugart: Thank you, Chair. I'll go as far as I can, given that the advice I give the government is necessarily between my minister and me.

I can't speak for other departments, but I can point to the fact that the Treasury Board itself has directives and policies in place that do apply to all departments, including HRSDC. It is the responsibility of departments to apply those in a manner that is relevant to their mission. For our part, we seek to do that.

I can tell you that there are mechanisms at the officials' level within the bureaucracy to review and stay on top of these issues, and to learn from any incidents that occur in order to adopt best practices and to continue to make the business culture of all departments as sensitive as possible to privacy and IT security. The Treasury Board does have a responsibility to update their policies and directives from time to time. That's, generally speaking, the regime that we live under.

Ms. Charmaine Borg: Thank you.

You did say that you have reformed your policies and the culture in which you treat personal information. I am happy to hear that. I'm really excited to see what's going to pan out and if we do dramatically see the number of data breaches reported fall to zero, which is ideal.

I'm curious to know what protocols existed beforehand and why there was data that was not encrypted when you're saying that shouldn't have happened. Where was the policy before?

● (1130)

Mr. Ian Shugart: Maybe I could start by asserting, as we may a number of times during this hearing, that culture is at the very individual level, so for all of this to work in a very large organization, all managers, all employees, have to be aware of the policies and directives, and they have to live it.

Ms. Charmaine Borg: Could I just ask how you ensure that?

Mr. Ian Shugart: We do that through training, and we have, as I mentioned, committed to upgrade our focus on training in this particular area. However, between training events the employees have to build it into their DNA.

Ms. Charmaine Borg: So what went wrong here?

Mr. Ian Shugart: In these cases, it clearly was not sufficiently in the DNA of the employees. That is what a business culture is, and our obligation is to facilitate the protection of information through the software and the hardware and the policies and to put in place the training.

I'm going to invite Mr. Parker to add to that.

Mr. Ron Parker (Associate Deputy Minister, Department of Human Resources and Skills Development): In response to your question, there were two particular policies that are relevant here: first, employees have a responsibility to report incidents; second, data that's sensitive should be encrypted before it's put on any particular portable storage device.

Ms. Charmaine Borg: So why wasn't this particular data set encrypted?

Mr. Ron Parker: As the deputy said, it seems the employees did not encrypt the data as would have been required.

The Chair: Your time is up. You took a little extra time to answer, and that's fine.

We'll now move to Dr. Leitch.

Go ahead.

Ms. Kellie Leitch (Simcoe—Grey, CPC): Thank you very much for taking the time to be here today.

As you've mentioned, Deputy Minister, for both ourselves as government members and for all of the opposition members here, this is a very serious concern. It is a very serious concern for all Canadians, particularly regarding their privacy and the direction and how it is treated.

As you mentioned, Deputy Minister, the minister has taken some action, whether it be upgrading the network for security practices or whether it be providing mandatory training, as you were talking about. I think we appreciate—I appreciate, at least—your sensitivity to this issue and how you and your colleagues are approaching it today.

I have a few questions. I'll go through them individually. Whether it's you or your colleagues who answer them, I think we're fine, as I think my opposition colleagues are of the same mindset: we want to get to the bottom of what occurred and address the seriousness of the issue.

With respect to the department and discovering this missing hard drive, what were the immediate steps taken? I know you outlined them in your notes, but as I was just reading through the notes here and following your dialogue, I noticed there was a bit of time with respect to when it was first brought forward and following that.

What was the immediate action? Also, what is the staff training to do that? You said part of it is culture. Obviously, we all have to take a little bit of individual responsibility for what we do, but what is that training? What was in place, and do those staff members now recognize the gravity of the situation?

Mr. Ian Shugart: Perhaps, Chair, I could respond to the honourable member's third question, and then Ron and Al can give the details on the other two.

I believe that staff are now very well aware. I think in an organization as large as ours one could expect—and I think it's the reality—that some staff are more aware throughout, and others are less aware or seized of the importance. Part of the focus on training being mandatory and being for all employees is to try to do our best to make sure there are no gaps, so that there is no employee in the department who can say he or she didn't realize that was the standard. If there have been such gaps in employee awareness, we want to close those gaps.

Generally speaking, I can tell you that in the organization we have taken some encouragement from the fact that employees have cooperated fully, including in the assessment of devices in the organization. We wanted our staff to be so concerned about this that they would drop whatever was necessary to drop in order to comply with the direction that we were going, but not so terrified that they would go underground. We believe that given the response of employees—their response in meetings and information sessions and so on—they have responded in that fashion.

I'll stop there and turn to my colleagues for the details.

● (1135)

Mr. Ron Parker: In terms of the immediate actions, initially the incident, as the deputy explained, was treated as a case of a missing asset—something to be found—with the belief that it was on the premises, still in the building.

As that set of searches became less likely, it pointed to a lower likelihood of the drive being found. Corporate security and the regional security officers were advised, which is the standard protocol. They began, then, a series of professional searches for the drive, and interviews were continued through the month of December into early January, when the likelihood of recovery of the asset seemed to be very low. At that point we launched a formal investigation that entailed professional investigators and we took the steps to begin to inform Canadians in early January.

The Chair: Is that it?

Okay.

Ms. Kellie Leitch: Similar to the comment the deputy minister had made before, we too find this completely unacceptable. We need to make sure that the privacy of Canadians is protected.

I think we all know the division of responsibility, with the policy side being taken in the House and the minister taking action. I know you've been involved and heard direction to make sure those things have taken place.

With the administration we took some action as well, and it also has some degree of responsibility of making sure that these things are implemented going forward to make sure we have a secure environment.

One of the items that has come up—and we've heard and talked about it—has been the involvement of the Privacy Commissioner and the timeframe for engagement in that, but also the engagement of the RCMP because of the seriousness of this matter.

Could you comment on when and who made the decisions with respect to engaging the Privacy Commissioner as well as the RCMP in order to make sure that Canadians were protected?

Mr. Ian Shugart: Mr. Parker referred to the protocols that we have, and I referred earlier to our standard, our approach, to the Privacy Commissioner's office.

As soon as we were aware of the likelihood of this information having gone and being not likely to be recovered, we knew, without any question, that the Office of the Privacy Commissioner needed to be engaged, and that's when we took that action.

It was in the minister's office that involving the RCMP and referring the matter to the RCMP was taken.

In the department, I might just say that we have absolutely no issue with that. That decision was taken on the basis of the seriousness of the situation we are in. It will be, of course, up to the RCMP to determine how they wish to deal with that request.

We will work in the appropriate fashion with the Privacy Commissioner's office for the investigation that they are undertaking and on anything that the RCMP decides to undertake, and on our own internal investigations to ensure transparency and openness and compliance with those investigations, and also to ensure appropriateness of information so that the integrity of any investigations that occur is not compromised.

● (1140)

Ms. Kellie Leitch: Thank you very much.

The Chair: We will now move to Ms. Charlton.

Go ahead.

Ms. Chris Charlton: Thank you very much, Chair.

Thank you to all of you, gentlemen, for being here before the committee this morning. I know it's probably not where you wanted to be on Valentine's Day, but thank you very much for sharing this part of the day with us.

Let me ask you this first, Mr. Shugart. Can you tell the committee what you understand “ministerial responsibility” to mean?

Mr. Ian Shugart: Ministers are responsible to Parliament, Chair, for ultimately all matters within their jurisdiction, including the policies of the government and the appropriate conduct of officials in their departments. By convention and in many cases by formal instrument of delegation, those authorities are delegated to departmental officials. That is often spelled out in the regulations to statutes and sometimes in the statutes themselves.

By convention, ministers are responsible for policy and officials advise ministers on policy. Officials are responsible for the administration of their departments.

Ms. Chris Charlton: Thank you very much, sir. You'll have heard our chair admonish my colleague that questions with respect to policy would not be appropriately directed to you today, which is why initially our request had been that the minister appear here.

You're quite right: you need to answer questions within the context of the administration of your department. In that context, let me try to ask some questions that you will be able to answer.

Can you tell me when a breach, in your ministry's understanding, is "totally unacceptable"? Those are the words that your minister used in response to questions that we raised in question period: that this breach was “totally unacceptable”.

The Chair: You can indicate what you think is totally unacceptable, but obviously not what somebody else might think.

Ms. Chris Charlton: No, but it's also in the notes that this breach was unacceptable, as my colleague pointed out.

Chair, seriously, we only have seven minutes.

The Chair: I know. What I'm trying to tell you is that we want to focus on the three issues before us. If your question to him is why he finds it totally unacceptable, he's entitled to answer it, but not what somebody else might have said or what you think they mean by that.

With that, you can answer her question. You understand what I'm saying.

Ms. Chris Charlton: Chair, with respect, this comes out of the presentation that's before us. The deputy said it was unacceptable, so let me follow up.

The Chair: I'm telling you that he can answer that with respect to his use of those words.

Go ahead.

Ms. Chris Charlton: Thank you, Chair.

Can you please—

The Chair: Well, let him answer.

Ms. Chris Charlton: Can you please tell me what, in the department's view, is an “unacceptable breach”?

Mr. Ian Shugart: I would say, Chair, that any incident involving the compromise of personal information is not acceptable. I cannot imagine, being informed of the situation of even one Canadian's personal information having not been properly handled or having been compromised, that I would say it is acceptable.

Ms. Chris Charlton: Thank you; we certainly agree on that.

However, we know from your testimony that there were 19 data breaches last year alone within your ministry. We know that there is no requirement for data breaches to be reported, so there are clearly a number of breaches that didn't fall into the same category as this, because it is only now that your department is strengthening its policies for the security and storage of personal information, according to the testimony you just gave.

I'm a bit surprised by that. In our community offices, where we have personal information for constituents relating to all kinds of health matters and passport information, we have protocols in place.

This is not the first breach in your ministry, nor in the government, and yet only now you're developing a new protocol. Can you explain why that is?

Mr. Ian Shugart: I don't believe, Chair, that I used the words "only now". I explained what we have done in response to this incident. Based on what we have learned from this incident, we have strengthened those policies, procedures, and practices.

I would not agree, respectfully, with any characterization that there were not policies in place in advance. Clearly there were; there are directives and were directives in place before. What we have done is to strengthen the protocols and strengthen the hardware and software rules and provisions in the system to further protect Canadians' personal information.

● (1145)

Ms. Chris Charlton: Let me remind you of another thing you said in your testimony. You said that employees were “asked if they had borrowed the hard drive”. It doesn't seem like a very strict protocol to me, if it's possible for employees just to borrow a hard drive with the personal information of over half a million Canadians.

Would you agree?

Mr. Ian Shugart: The questions, Chair, that we put to employees were intended to canvass all possibilities about what may have happened. We included among those possibilities inappropriate handling of the hard drive.

That was in no way intended to suggest that we would find that behaviour acceptable. Indeed, the questions were not intended to assume anything about what had happened. We were simply being exhaustive in our questioning of employees to elicit any information we could about what had happened.

Our priority in that situation was to recover the asset and the information that it contained. That was the purpose of questioning. In no way does it imply that we would regard any such behaviour as acceptable.

Ms. Chris Charlton: In the age of technology, if somebody has access to this information, they can misuse that information in a matter of seconds electronically.

One thing you indicated is that the Privacy Commissioner was contacted a week after you first discovered the breach with respect to the USB key. What is your protocol around how long you will wait to see whether it miraculously turns up somewhere before you think you need to notify someone that the breach has happened?

Mr. Ian Shugart: We certainly don't depend on miracles. We were being diligent about the search, and when we came to the conclusion or the strong supposition that the material was not likely to be found, you'll recall that I said we continued even after that to search exhaustively. We informed the Privacy Commissioner at that point.

Ms. Chris Charlton: Who do you inform first, the minister or the commissioner?

The Chair: Your time is up, but go ahead and finish.

Mr. Ian Shugart: I informed the minister quite early on that we were engaged in this search, and we kept the minister informed about the involvement of the Privacy Commissioner and about every critical step of our investigation and about what we were learning as we went.

Could I ask my colleague whether there's anything that he would want to add to those facts?

The Chair: As I mentioned, the time is up, but go ahead and answer that before we go to the next questioner.

Mr. Ron Parker: On the Privacy Commissioner side, we informed the Privacy Commissioner's office on December 14, followed up with a written contact on the next Monday, and have consulted the Office of the Privacy Commissioner throughout the piece to work to find the appropriate ways to manage the incident and to inform Canadians.

The Chair: Thank you.

We'll now move to Mr. Mayes.

Go ahead, for seven minutes.

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

Thank you to the department for being here today. I appreciated your opening statement that the loss of this information is not acceptable and that your department recognizes that. We totally agree.

One of the issues I have is that you made a decision to inform the RCMP of the loss of this data by the department. Did you consider, after you did the searches, that you had moved from misplaced asset to a missing asset to actually a possible theft of an asset? If so, who made that decision to call on the RCMP?

Mr. Ian Shugart: We did not make any assumptions, and even now we have not made assumptions, about precisely what happened. That is why investigations have been undertaken, including our own internal investigation.

We can say—and the committee will appreciate that it's not possible to prove a negative—that we encountered no evidence of malfeasance, and none of the monitoring that has been done since has given us any reason to believe that malicious activity has been undertaken, but that in itself does not deal with the seriousness of the incident. Given the numbers involved, the decision was made—I think not unreasonably—that the RCMP should have that information and be asked to consider their response.

● (1150)

Mr. Colin Mayes: Thank you.

For these types of breaches of security and procedure by employees, is there a policy in the department on consequences for any breach of the security procedures by the department?

Mr. Ian Shugart: Indeed there is. The obligations of employees, Chair, in regard to the handling of personal information are set out in the code of ethics. There's a standard code of ethics for the public service overall, which is in the domain of the Treasury Board, and then each department takes that foundational code and applies it to its own mission, its own circumstances, and makes it precise.

In our case, as I've indicated, protection of personal information is so critical to our mission that it is in our code. Employees are required to abide by the code in all aspects of information and so on. Breaches of the code of ethics are considered on a case-by-case basis, and disciplinary action for breaches can include termination. Should there ever be an incident that involves criminal elements, then obviously penalties outside the department's responsibility for public service discipline would come into play through due process of law, etc.

Mr. Colin Mayes: The department moved forward quickly to ensure the integrity of the credit and the information of those who had their information compromised. Can you give us an update? Have there been any problems? Have you seen any indication that anybody has used this information? What sort of feedback are you getting from those who have concerns? Have you set up some sort of system to receive calls and reassure those who are included in the numbers that have been compromised?

Mr. Ron Parker: The principal way of dealing with this is through the contract that we have established with Equifax.

About 50,000 affected former students have enrolled in that service. We have no evidence thus far that there has been any fraud or other inappropriate activity. There is a special 1-800 number that is set up for affected clients to phone. We have not had any calls indicating fraud has been observed.

In addition, we have established notations in the social insurance registry so that each social insurance number has a special notation that the client was potentially affected by the incident. In the event that the national identity service's centre receives a request to change the social insurance information or request a card, a special flag will come up and the client will be requested to provide the appropriate identity documents and photo identification.

We have looked back to what has been happening with the social insurance registry prior to and after the loss of the information and there has been no change in the pattern of requests or the nature of requests that have come in.

● (1155)

Mr. Colin Mayes: There's a lot of information you deal with. Do you have any figures on the volume? It's horrendous and it's a big challenge, and especially with communication today, these challenges.... We're adjusting to them. I'm on the committee for ethics and privacy, and we're going through a study on that and we understand some of the challenges we're facing with breaches of privacy, not only as government but also in society. It's pretty challenging.

In the department, do you have an ongoing program to review all the procedures and information—the firewalls and all those kinds of things—to keep up to date?

The Chair: If you could keep it relatively brief, we'll maybe pick it up a little later. Go ahead.

Mr. Ron Parker: Thank you, Mr. Chair.

Overall in the major programs that HRSDC administers, there are about 28 million clients per year who are in our databases. We deal with roughly 84 million transactions per year across those major groupings, including Canada Student Loans, the Canada education savings program, the Canada Pension Plan, old age security, and employment insurance. We have a lot of transactions and we have a lot of Canadians as clients. In terms of their—

A voice: We'll skip that.

Mr. Ron Parker: Okay. We'll come back to it.

The Chair: You'll come back to it? Okay.

Did you wish to make a short comment, Mr. Shugart? No. We'll come back to that.

We'll turn it over to Mr. Cuzner. Go ahead.

Mr. Rodger Cuzner (Cape Breton—Canso, Lib.): Thanks very much, Mr. Chair, and I thank the gentlemen for being here today.

I have only seven minutes and I'm going to try the best I can to get all my questions in. You guys have been pretty direct, and I appreciate that. If you can, continue that, and if I cut you off, it's not bad manners; it's just that I'd like to get the questions in.

First, my questions are going to focus on those who have been impacted, on those who held loans. Can you guarantee that it's only those between 2000 and 2006 who have been impacted? Are you confident with that?

Mr. Ron Parker: We've examined the data carefully. There are some former students outside of the 2000-2006 period, about 2,800 students overall. They fall mainly in 2007. There are about 2,600 students in 2007, and after—

Mr. Rodger Cuzner: I appreciate that. We are getting them from 2007. Thank you very much.

On parental information, is there information on the parents or spouses out there, as well as about the students?

Mr. Ron Parker: No, there is no information on the parental side.

Mr. Rodger Cuzner: You're comfortable that there's no parental information out there, and no information on spouses. Great.

Do you have a number for how many Canadians have reported concern about loss of identity or loss of information?

Mr. Ron Parker: We have answered 200,000 calls overall, and of that amount in total, about 65% are affected clients. Prior to the notification letters going out, it was running about 50-50 in terms of affected students versus non-affected students, and since that time, since the letters were received, the contacts have been—

Mr. Rodger Cuzner: If I could just offer some advice, some of the calls we got from students say that the Equifax people aren't really confident with the information that they're sharing, so just as a tip to you guys, please make sure that these agents for Equifax are continually briefed or given the best information you can.

A corporate example is Sony International. A similar breach happened with them back a number of years ago. For all of the millions who were impacted, Sony picked up the tab under the categories of alert, monitor, and ensure. They provided a fraud alert, credit monitoring, and an insurance of $1 million coverage for each person. Had their identity been stolen, Sony would ensure each person for that amount.

Let's say that's over on this side of the continuum. The department's response would be anywhere from doing nothing to the Sony model. Where do you feel your response has been within that continuum?

● (1200)

Mr. Ron Parker: We feel that the response is appropriate and that it is a strong response. It's a two-fold response through the contract with Equifax. The specialized, customized contract that we have will flag any attempt to increase credit or change credit information, and coupled with the monitoring of the social insurance registry—

Mr. Rodger Cuzner: I have a concern when we look at the Financial Consumer Agency of Canada's website and when we look on the federal Privacy Commissioner's website.

They say on the website that if an organization has collected your personal information and they notify you that a data breach means there's a risk that you will be used by identity thieves, then protect yourselves. They say to contact the fraud departments of the two major credit bureaus, request a fraud alert be placed on your files, order copies of your credit report, and repeat this step each six months.

You have used Equifax. Why have you not used TransUnion as well?

Mr. Ron Parker: Mr. Chair, we are exploring the possibility of arrangements with other credit bureaus and financial institutions.

Mr. Rodger Cuzner: On the Equifax deal, those services are provided free of charge in eight out of ten provinces. I understand they are. Are you giving a special service beyond what is normally free of charge in eight out of ten provinces? Could you expand on what it is you're providing over and above that?

Mr. Allen Sutherland (Assistant Deputy Minister, Learning Branch, Department of Human Resources and Skills Development): I'd be happy to, because there has been a lot of confusion on this issue.

Some people have been confusing the lost wallet service with the customized credit alert package that has been prepared by Equifax for the department. There are some important differences. For one thing, the lost wallet service is not available across the country, but more importantly, it provides a lesser standard of service. For instance, the lost wallet service is only available for three months. The service we've purchased from Equifax is the industry standard of six years.

The second thing is that the lost wallet service doesn't provide prevention or fraud mitigation for clients the way the credit alert system does. What the credit alert service does is notify the credit grantor that the person's ID has potentially been involved—

Mr. Rodger Cuzner: Perhaps I can interrupt, and I apologize, but Equifax had told us this is in fact free of charge to all consumers.

The Chair: Mr. Cuzner, you're at your seven minutes. Please put a quick question. Otherwise, we'll move on.

Mr. Rodger Cuzner: What is the total cost of the Equifax package to cover the 600,000 people?

Mr. Ron Parker: The contract with Equifax and its value are commercially confidential. The reason the cost is commercially confidential is that the competition would be able to break it down to a per-unit cost. Thus, we've agreed to keep it commercially confidential.

The Chair: Your time is up.

We'll move to Mr. Daniel, and after that we'll take a quick break and start the second round.

● (1205)

Mr. Joe Daniel (Don Valley East, CPC): Thank you, Mr. Chair. Thank you, witnesses, for being here.

Again I have to say it's obviously a very difficult situation to lose data like this, and so I can sympathize with the people whose data has been lost.

One of the things that's important to understand is the root cause of all of this. The root cause will help you come up with the best solution, in my opinion.

My question is this: why was this information allowed to be copied from a server to an external device, and what was the department's policy at this time on portable devices like this?

Mr. Ron Parker: According to policy, the data should have been encrypted before it was copied to any portable device, and clearly it was not. The policy is there. The investigation will look at why it was not encrypted and the steps to look further into what the issues were.

Mr. Joe Daniel: Has this loss of data brought about any other significant policy changes on how the department handles Canadian information? If so, how will these changes prevent a similar situation from recurring?

Mr. Ron Parker: The changes we've embarked upon are critical and key. It will be night and day in terms of the level of protection.

First, with respect to the information hardware, all of the USB keys that we—

The Chair: Go ahead, Ms. Borg.

Ms. Charmaine Borg: Mr. Chair, you so kindly reminded me during my testimony that I had to specifically speak to the three items on the motion about this particular data breach, and his question was not about this particular data breach. If you're going to implement that standard, I think you should implement it for all members of the committee.

Thank you.

The Chair: Fair enough. I took the question to relate what you're doing with respect to the action you're taking following this breach. Now if we're mistaken on that, then it's another matter, but it's certainly appropriate to talk about what some of the long-term solutions are and what actions you've taken.

Ms. Charmaine Borg: Then it's appropriate to talk about the situation in general? I think it is.

Mr. Joe Daniel: No, this is specific to the policy of the department. That's the question. It relates directly to what's being talked about.

The Chair: Go ahead.

Mr. Ian Shugart: I think, Mr. Chair, we understood the question to be an elaboration of the measures that we have taken in response to these incidents which, as I understood it, was included in the order.

The Chair: That's the idea, but answer it within those confines. If members still find that objectionable, raise your objection.

Go ahead.

Mr. Ron Parker: Only approved USB keys will be allowed, and the department is acquiring a large number of encrypted USB keys. As a result, portable hard drives are no longer allowed to be plugged into the network, nor are personal devices that use a USB connection. We are monitoring the network and accessing the network on a regular basis and moving to ensure that none of these devices are connected, which is a big step in preventing the movement of data off of the network, which is encrypted.

The other significant measure is the implementation of the data loss protection software. This will tell us exactly what sensitive information is on the network, where it is, and how it's stored, and it will allow us to take appropriate measures to make sure it's secure.

I repeat, the network is encrypted. It will also allow us to deal with the movement of the data. We can control or prevent the movement of data once this software is in place. These are very important measures that we're taking in response to the incident.

Mr. Joe Daniel: Are there any measures you're taking to constrain how much data can be put on any one USB at a time, or anything like that?

Mr. Ron Parker: We have not looked at that particular issue at this time.

● (1210)

Mr. Joe Daniel: Okay.

What guarantees can you offer my constituents that this data will not be used fraudulently as a result of this error?

Mr. Ian Shugart: Mr. Chair, I don't think we can ever offer guarantees. What we can offer is the assurance that, as Mr. Parker has said, we are monitoring things extremely closely, both through the Equifax arrangement and through the annotations in the social insurance register, to spot any suspicious activity that could give rise to suspicion. That suspicion alone would be the basis for the individual and for HRSDC to take appropriate action.

Again, quite obviously we are very pleased that we have absolutely no indication at this point of malfeasance or of misuse by any third party of any of this information.

Mr. Joe Daniel: For my colleague across the way, we talked earlier about using TransUnion and Equifax, but you've chosen to use just Equifax. Can you help me understand again why you're just using one of the credit companies?

Mr. Ron Parker: I'm afraid the answer will be very similar. We're exploring the possibility of engaging with other credit bureaus and financial institutions to gain incremental services. At this moment, that's all that we can say about where we are.

Mr. Joe Daniel: But pretty much all the clients will be serviced by Equifax.

Mr. Ron Parker: At the moment, yes, the contract is with Equifax.

Mr. Joe Daniel: Thank you very much.

The Chair: Thank you for that.

With that, we've concluded the first round of questioning. We'll take a brief five-minute suspension of proceedings and then come back here so we can complete the second round.

● (1210)

(Pause)

● (1215)

The Chair: If we could get the members back to their seats and get department officials, deputy ministers, and associate deputy ministers back to their tables, we'd like to start if we could. If we could get you back to the table there, that would be good. We'd like to complete a second round if that's possible.

We're going to start our second round of questioning. I believe we're going to lead off with Madame Boutin-Sweet.

[*Translation*]

Ms. Marjolaine Boutin-Sweet (Hochelaga, NDP): Thank you, Mr. Chair.

Thank you, gentlemen.

We have not talked a great deal about the protection for those you call “clients”. I for one will use the term “former students”. We are also talking about 250 employees, but we often tend to forget them.

The minister said that you contacted the people whose information was up to date. We are talking about half a million students or former students. So they are people who move a lot.

How many of those people were you able to reach?

Mr. Allen Sutherland: We contacted approximately 320,000 people.

● (1220)

Ms. Marjolaine Boutin-Sweet: In other words, 200,000 people still don't know that they might have problems. If those people were victims of identity theft or some other issues, those problems might still come up, especially if this happened in December before the whole situation was released in the papers.

Mr. Ron Parker: That is why we put out announcements, posted documents on our website and made efforts to have this out in the media in order to be able to contact the students whose current information we didn't have.

Ms. Marjolaine Boutin-Sweet: You also said that there were 300,000 calls. So that means that 200,000 people perhaps didn't call or see those announcements and they don't know that their personal protection might be at risk.

Mr. Ron Parker: There have been 200,000 calls so far. As Al said, we sent 326,000 letters. Some of those people may still contact us.

Ms. Marjolaine Boutin-Sweet: Could you tell us more about Equifax? As Mr. Sutherland said, it is complicated. I would like you to be very clear about what is being offered to people. First, do the students need to make a request? What do they get? Who pays for what? What types of services are we talking about? Is it just a notation on their credit files, or do you have a surveillance and oversight system in place? Could you make this clear for me and everyone here today?

Mr. Ron Parker: The students have to call the call centre to have access to the program. They have to opt in for the protection of their private information. That is the only way to do so safely.

In terms of services, we have a customized package for our clients. There is a notation on the Equifax file that tells financial institutions that people's privacy may have been compromised. In those cases, the financial institution will ask clients to provide additional proof of identity if they want to increase their credit limit, to get a new credit card, or for any other transactions like that.

In addition, as mentioned, there is a call centre specifically for our Equifax clients. Those services will be provided for six years. After six years, we will have to review the situation closely.

Also, we have added notations to the social insurance numbers that might have been affected. For any changes to social insurance numbers, additional proof of identity will be requested.

● (1225)

Ms. Marjolaine Boutin-Sweet: Based on what you are saying, a notation is made on credit files, but there is no oversight. In other words, no one will check to see if the social insurance number has not been used by someone else somewhere to get a loan or to apply for credit cards. In fact, neither the government nor Equifax will provide any surveillance.

Mr. Ron Parker: Not exactly. The two are actually independent from each other.

The people in question are clients of financial institutions. When they make a request to obtain additional credit or a mortgage, or to increase their credit limit, the institution will see the notation on their Equifax file indicating that they might have been involved in an incident. According to their protocol, financial institutions will then be able to ask for additional proof of identity.

Ms. Marjolaine Boutin-Sweet: I have not received an answer to my question about costs—

[*English*]

The Chair: Thank you, Madame Boutin-Sweet—

Ms. Marjolaine Boutin-Sweet: I already asked this question.

The Chair: —your time is well up. Sometimes you don't always get the answer you want or like the way it comes out, but your time is up. If Mr. Parker wishes to elaborate somewhere along the way, he can, but we'll move now to Mr. McColeman.

Mr. Phil McColeman (Brant, CPC): Thank you for coming today to deal with a most difficult—and the word's been perhaps overused, but I'll state it again—a most unacceptable event.

It reminds me of risk. One comment Mr. Shugart made was that you can never give absolute guarantees. There will always be risk. There was a level of risk before this happened, and now perhaps another level of risk afterwards because of the new protocols that are put in place as a result of this situation. It reminds me of 9/11 and what happened in terms of our feeling secure after 9/11. The world changed. We had to put a lot more security in place.

Having said that, I'm interested to know the protocols that were in place at the time that these devices went missing with this important information about Canadians. Were the protocols for the handling and storage of that information followed?

Mr. Ian Shugart: My colleagues can elaborate, but subject to anything we may learn in the investigation, it seems to us that given the requirement for encryption and the fact that the information transferred was not encrypted, it's pretty clear that the policy was not followed.

The policy was in place and the requirement was in place, but the indications we have are that the policy was not followed.

Mr. Phil McColeman: Would that include your policy regarding storage and the place where they were stored? We're told it was in a locked cabinet. Was that the proper protocol for where backed-up hard drives should be placed?

Mr. Ron Parker: The devices are to be stored in a secure locked cabinet. The investigation will look at what the circumstances were when that the device, the hard drive in particular, was not in that locked cabinet.

At one point we knew that it was, right? The evidence points to it being in the cabinet. What we know is that it's unaccounted for at this time, and we are looking to understand how that came to pass.

● (1230)

Mr. Phil McColeman: You mentioned in your opening remarks, and it's been mentioned here in our questioning, that the level of consequences for not following protocols goes right up to and includes termination.

What actions are being taken?

Mr. Ian Shugart: Chair, first I need to say that we don't have the results of the investigation with respect either to certainty about the individuals involved or the circumstances. Therefore, to go further than that would be conjecture. Mr. McColeman will understand that I won't do that.

I can say, however, that a number of things would be taken into account in such situations with respect to what discipline is appropriate, including the genuine awareness of the individual employee. Responsibility by a manager, for example, would be expected to be greater than that of an employee, and an employee who deals constantly with this kind of information would have a greater expectation of compliance than one who was unaccustomed to it. These are all illustrations of that factor, that criterion of awareness.

Motivation—the intent of the individual—is clearly a factor in any decision about discipline. Again, I won't theorize in this situation, but intent is clearly a factor. The gravity of the situation is a factor, as is the degree of remorse of an individual and the willingness to comply. We would take all of that into account in deciding each individual case, based on what we know.

Of course, one has to have clear knowledge before acting on the basis of discipline. We would take all of that into account in deciding where on that continuum an appropriate action would be taken.

Mr. Phil McColeman: I appreciate your articulating it in those terms of taking the broad range of circumstances, and I suppose, cultural influences, into consideration.

I think that on both sides of the political spectrum, we all recognize the gravity here. There has been some mention, I think by the minister, that because of the gravity and the seriousness of this situation, in the go-forward situation and the establishment of new protocols and procedures, there will there be an increased toughening, shall I say, of the consequences, should this happen again.

Mr. Ian Shugart: Again, I don't want to stray too far, Chair, into the realm of conjecture, but I think I can say that as a consequence of deepening our culture and our training and our awareness of these issues, one ought to be able to expect a higher standard in the future.

As I indicated before, the code of ethics includes both the range of disciplinary action that can be taken and the obligation for personal information protection. To the extent that we deepen the cultural awareness and the rigour and the extent of the training and so forth, in this issue particularly we will be able to raise the awareness and commitment of employees. I have to say that of course we have many areas where public servants have mandatory obligatory training, and that is appropriate. As our CIO knows only too well, and we all do as managers, the area of information technology security and information management is itself becoming more and more complex and broad and intertwined, and in order to achieve that desirable state of culture that I've referred to here, we do need to raise our game in terms of awareness and commitment of employees.

Against that backdrop, I think that employees should expect that we will be going about this in a strict fashion.

● (1235)

The Chair: Thank you, Mr. Shugart.

We'll now move to Mr. Cleary for seven minutes.

Mr. Ryan Cleary (St. John's South—Mount Pearl, NDP): Thank you, Mr. Chair.

Mr. Shugart, I reviewed your speaking notes and the timeline for both incidents, and my first question is in regard to the timeline.

In the first incident, which was November 5, we have a missing hard drive with the information on 583,000 Canadians, the student loan information. It was reported to the privacy commissioner on December 14. That was more than five weeks after this device went missing. In the second case, the USB went missing on November 16 and the privacy commissioner was notified six days later.

Why did it take more than five weeks in the first case—what I would describe as the more serious case and the one that affected more Canadians—and six days in the second case? Why?

Mr. Ron Parker: I think the reason is that from the early days—from the November 5 period to the end of November, roughly—we were looking for an asset. What was on that asset was not well understood. The extent of the information that was on it became clear on December 6. At that time we began to react swiftly, in terms of the actions taken. The searches intensified, and, as I mentioned, the privacy commissioner was notified as of December 14.

Mr. Ryan Cleary: Mr. Parker, I'll stop you there. I've got to ask this question.

You describe the actions as “swift”. You say you acted swiftly, but on November 5 this first hard drive went missing, and there wasn't an informal investigation launched until the first week of January. How can you describe that as “swift”?

Mr. Ron Parker: The search for the hard drive and the security incident protocols call for corporate security to become involved. That took place on November 28, once the management of the department was notified. At that time the protocols kick in and the notification up the line takes place and we became aware of the incident.

Until that time the employees were looking for a hard drive. As of December 6, in terms of moving quickly, once it became clear that we were dealing with 583,000 lost records of students and the information for 250 employees, we had a short time between that and the notification of the Privacy Commissioner. We intensified the search, and once that was done and we came to the view that the likelihood of finding it was low, we notified the Privacy Commissioner.

Mr. Ryan Cleary: Mr. Parker, I'm sorry to interrupt, but I want to get a few more questions in quickly.

I know that the minister and the officials here today have described the potential security breach as unacceptable, but on the department's response to the loss of a hard drive and USB port, would you also describe that and the timeline here as unacceptable?

Mr. Ian Shugart: No, I wouldn't, and I don't want to be misunderstood as in any way saying that what occurred was acceptable. It wasn't, but with the information we had at the time that we had it, we believe we acted appropriately with respect to our protocols for the Privacy Commissioner.

We were continuously searching for the assets. At the same time that we became aware of the content, we immediately began the process of informing people and putting in place throughout that period the additional measures—hardware, software, and so on—for prevention of such things in the future. On all three of those paths we were proceeding, we believe, appropriately, given the gravity of the situation, which we do not in any way question.

● (1240)

Mr. Ryan Cleary: I have two requests as well. In terms of a hard copy—you probably wouldn't want to give this on a USB port or whatever—of the new policies and procedures on the handling of personal data, can this committee be presented with a copy of your new policies?

Also, are you prepared to give this committee a copy of the report into your investigation into both of these incidents?

Mr. Ian Shugart: Chair, as to the first, I will undertake to provide the committee with whatever information the committee asks for.

With respect to the second, I will provide any information that we can that is not precluded by the statutes of Canada.

Mr. Ryan Cleary: At what point—

The Chair: Mr. Shugart—

Mr. Ryan Cleary: I have one quick question.

The Chair: Okay, but before we get to that question, we should probably resolve what you're asking for.

With respect to the first of the two requests, you're saying it's up to the committee to decide if that's provided. On the second request, you will provide the information. Did I get that right?

Mr. Ian Shugart: I'm sorry, Chair; I'm having a little trouble understanding the back and forth here.

The Chair: Okay. Mr. Cleary, you requested two things....

Mr. Ryan Cleary: Yes, I requested two things: a copy of the new policies and procedures on the handling of personal data be presented to the committee—

The Chair: Mr. Shugart, your response was....?

Mr. Ian Shugart: I will provide the committee with anything the committee asks for.

On the second request, which specifically was the investigation report, I'm anticipating that there may be some elements of that report dealing with individuals that I may not be able to share with the committee because of legal limits, but I will be as forthcoming as I can.

The Chair: Here's what we'll do. If you want to put forward those two specific items for production in terms of a motion, we will deal with that as a committee after you've left and make a decision on that, but we won't interrupt the flow of evidence.

Did you wish to put that in the form of a motion?

Mr. Ryan Cleary: Sure.

The Chair: Okay. Then we'll deal with that after you have left, but we'll continue with your questions.

We did stop your clock, so go ahead.

Mr. Ryan Cleary: Thank you, Mr. Chair.

Just so I understand this correctly, in terms of the missing hard drive and in terms of the missing USB port, did they both go missing from the same building in Gatineau?

Mr. Ian Shugart: No.

Mr. Ryan Cleary: It was different buildings.

Mr. Ian Shugart: Yes.

Mr. Ryan Cleary: At what point was the RCMP called in to investigate?

Mr. Ron Parker: Do you have the date?

Mr. Ryan Cleary: I am going to move to another question and you can answer that in a minute.

One thing that was pointed out, Mr. Shugart, in your opening remarks was how there's protection here for a potential privacy breach for six years. Then in another question, I think Mr. Daniel asked you about whether there could ever be guarantees that personal information won't be used nefariously, and the answer was that there can never be guarantees. My question is this: what happens after this six-year timeframe that you've outlined? What happens after that?

The way I understand it, these 583,000 Canadians in the first case and the 5,000 in the second case are potentially going to be looking over their shoulders for the rest of their lives, so what happens after six years?

Mr. Ian Shugart: We do not preclude, Chair, that the period could be extended. We will be monitoring and evaluating at that time what has occurred over this period. On the basis of a risk assessment, we do not preclude that it would not be extended.

The Chair: Your time is up, Mr. Cleary. Thank you very much. We didn't interrupt for a discussion on the motions in respect to your time.

We will now move to Mr. Butt, but before we do that, if you have an answer to his previous question, go ahead.

● (1245)

Mr. Ron Parker: The minister's office notified the RCMP on January 7.

An hon. member: Was that in both cases?

Mr. Ron Parker: No, it was only in the one case.

The Chair: All right. Is that clarified?

We will then move to Mr. Butt.

Go ahead.

Mr. Brad Butt (Mississauga—Streetsville, CPC): Thank you very much, Mr. Chair.

Gentlemen, thank you all for being here today. I have very much appreciated your straightforwardness in this matter, your candour in responding to the questions, and the wholesome way that you've approached this issue, which we all agree is completely unacceptable. There's not a single person in this room who doesn't believe that these two incidents were completely unacceptable.

I appreciate the approach the department has been taking in dealing with this situation. I'm one of those who believe that you also have to look beyond an incident or incidents like this to ask what we are going to do to make sure it doesn't happen again.

What are we going to do to improve our safeguards and our processes and procedures? That is the line of questioning that I'm going to go with: where do we go from here—how to get to zero, as we say it is our goal to do?

I want to get you to comment quickly, to reiterate the direction that the minister has given to you, which as I understand it is to review the ways that employees handle Canadians' data, fix any gaps that allowed this to happen, update network security practices to prohibit external hard drives, and provide more mandatory training for all employees in the proper handling of sensitive and personal information and on the new security policies.

Is that the direction, Mr. Shugart, that you are taking from the minister in what you are doing on a go-forward basis now?

Mr. Ian Shugart: Yes, it is indeed.

I would also indicate that we are open to the advice of the Office of the Privacy Commissioner for any additional advice that may be forthcoming or actions that we should take. Similarly, we have consulted with third party experts in the industry. We are open to advice and best practices from any quarter that can help us achieve the standard we are after, but yes, that is the direction.

Let me indicate two particular areas. The data loss protection software that will be put in place, as I understand it—and my colleague the chief information officer can correct me if I wander into the swamp—will be deployed throughout our system, allowing us to monitor when there has been any inappropriate transfer of data. That's built right into the software. The system can be designed such that the folks who monitor such things will know when, in effect, a flashing light goes on and says that data has been transferred in an inappropriate way, against the protocol or the standard. We would then be in a position to go in and ask, in a very precise area, why that data was transferred in a way that's not appropriate.

That's a technological response, but what we're after is avoiding any inappropriate handling or transfer of data in the first place. The very merit of our institution is founded on human dignity—that's why we protect individuals' information—and concern for human beings, and that's why we have the programs we do.

The other side of that coin is that human beings run the system, and there can never be any absolutely fail-safe system. However, in terms of that human culture, we want to be an organization that is excellent in everything we do, one in which individuals know their part in the larger scheme of things and will handle Canadians' information carefully and sensitively and according to the rules.

That's what we're after, and that's the direction in which we're going.

● (1250)

Mr. Brad Butt: Did you want to add something, Mr. Parker? Go ahead.

Mr. Ron Parker: Let me pick up on one of the first points you made with respect to examining current practices.

With their employees, each assistant deputy minister in the department is examining their practices around the movement and storage of data. Employees, I believe, are taking these incidents as seriously as we are, and we are pursuing in nitty-gritty detail exactly how information is stored and how it is moved branch by branch within the department, right down into the trenches.

This is a very intensive process. We're meeting with each unit throughout the department and looking at what they're doing in the verification of their data or inventories and how they're storing that information.

Mr. Brad Butt: Can you expand on the measures the minister commented on for the tougher consequences for employees in the future, should they not abide by the new policies? What are some of the likely outcomes that may take place, should this kind of breach in protocol happen in the future?

I'm assuming that part of your plan will be intensive training and reminding all the employees in HRSDC of what the rules and protocols are, but you may come up with a situation in which a breach has been caught yet again. We all hope not, but if we do, what are some of the likely consequences that you would be administering?

Mr. Ian Shugart: Mr. Chair, Mr. Butt will know that I won't enter into the hypothetical, but the range of potential, at the one end of the spectrum, is of course termination, and that is explicit to staff in the policy and in the code of ethics. That obviously is a very severe measure and has to be justified concomitantly by severe behaviour.

Beyond that spectrum, if there is any malfeasance involved on the part of the employee—and sadly, we know that in the public service's history there have been occasions when criminal behaviour has been undertaken—the full force of the law is available and waiting to deal with any such situation.

The Chair: Thank you. If you have a short closing comment, make it, and then we'll move to Mr. Cuzner.

Mr. Ian Shugart: I would say that throughout that spectrum, for individuals who are part of the "pay at risk" system, that element would be brought into play. Behaviour in this area could play into decisions about promotion and advancement, and there are measures such as suspension that can be a part of that arsenal of discipline.

The Chair: We'll move to Mr. Cuzner. It's for seven minutes.

Mr. Rodger Cuzner: Thank you.

Just to reiterate my comments from my last questioning with regard to Equifax, if you could be vigilant on this to make sure that Equifax is very much up to speed, I know that those engaged would appreciate it.

The other thing is with securing TransUnion; you indicated that you're weighing that possibility. We see the federal Privacy Commissioner suggesting that this is where we should be and the Financial Consumer Agency of Canada recommending it. Know that I strongly advise that you make sure that this protection, to at least.... What we're trying to do now is alleviate some of the concern for the 600,000 people who have been affected.

You indicated in your remarks, Mr. Shugart, that 250 employees were affected. Is the coverage those employees have been offered the same as for the 600,000?

● (1255)

Mr. Ron Parker: It is the same. We've been in touch with the employees formally by letter and have offered exactly the same services.

Mr. Rodger Cuzner: Thank you very much.

I had offered the example of Sony's taking out the insurance policy on those impacted by their breach. I would think the answer to whether you guys have insurance would be that the Government of Canada is its own insurer. Should someone have their information stolen in this case and end up with a degree of financial loss, is the government willing to cover the cost of that loss if it can be proven that security was breached or was a result of that breach? Are we there?

The Chair: Again, it's up to you whether you answer that or not. What the government will do is obviously not in your purview, and it's hypothetical. In essence it's....

If you have a comment, go ahead. I just want to warn you.

Mr. Rodger Cuzner: Can I ask if the department is going to do it, Mr. Chair?

Mr. Ian Shugart: I was just going to say, Chair, that I don't want to be evasive, but I think I have to regard that as hypothetical. I wouldn't be comfortable in venturing into that area at this stage.

You indicated "should" something happen, and "if". Let me just say that our action plan involves very careful monitoring at our end and via the service provided by Equifax, and we will be following this very carefully.

Mr. Rodger Cuzner: So the department would not be in the process.

Mr. Ian Shugart: I'm not in a position to speak hypothetically about what the government would or wouldn't do in a situation—

Mr. Rodger Cuzner: So you wouldn't be preparing a contingency in that regard?

Mr. Ian Shugart: Well, the circumstances itself are hypothetical, and I'm not in a position to comment on that area. I just don't want to venture into that hypothetical realm at this stage.

Mr. Rodger Cuzner: Mr. Sutherland, we've been in contact with Equifax since the last round of questioning. A very senior member of the company has assured us that what the students are getting is exactly the same as the average Joe gets, which is free of charge in eight out of ten provinces.

Draw me two columns. Tell me the difference between the two types of coverages, the one that's free and this special design you guys have.

Mr. Allen Sutherland: My information is also from Equifax. Maybe it's something you need to work through with Equifax. The discussions we've had have been very direct and have been senior as well. The lost wallet service is a service that is not available nationally. It's not available—

Mr. Rodger Cuzner: I had indicated that—it's available in eight out of ten provinces—but it does extend for six years.

Mr. Allen Sutherland: My understanding and what they've told me is that it extends for three months.

Mr. Rodger Cuzner: It's six years, but that's okay.

The Chair: Carry on.

Mr. Rodger Cuzner: What are the other differences?

Mr. Allen Sutherland: The other difference is the lost wallet alert is of a different standard than the credit flag. The credit flag requires the credit grantor to ask additional questions requiring enhanced authentication, which is different from the lost wallet service, which doesn't have the same requirement and compulsion to it.

Mr. Rodger Cuzner: I'm sure they just ask for an additional piece of ID with the lost wallet.

Mr. Allen Sutherland: My understanding from Equifax is that the requirement is higher. In addition, too, there are the customized services we're getting with the client services, whereby they will take time to explain the service and the options that folks may have, including taking off the service and what they may do to improve. It's a package of services that we've purchased.

We've asked Equifax a number of times, because we have heard the comment out there that you've heard as well, and they have assured us that the package of services that we've provided is significant. It is something that has a cost attached to it, and it is not the same as the lost wallet service.

● (1300)

Mr. Rodger Cuzner: I would see the cost....

Have I got a couple of minutes, Mr. Speaker?

The Chair: You have about 30 seconds.

Mr. Rodger Cuzner: Could you provide us with the detail? I would think that the specific package would be the additional information, but I don't see any additional protection for the people. I'm not certain that's what's taking place here. I can see the additional client interaction that we could focus on and maybe try to improve as being a cost. Could you provide us with a parallel comparison between the services?

The Chair: Thank you, Mr. Cuzner.

I think if you want to get the comparison of those two, you could make it the point of a motion. We have one to deal with the provision of other information and we can deal with that after these gentlemen have left. Do you want to make that a motion to be discussed by us, Mr. Cuzner?

Mr. Rodger Cuzner: Sure.

The Chair: I see that we had Dr. Leitch on the list for questioning, but our time has unfortunately run out and we have a motion to do with.

Gentlemen, first of all I would like say thank you for coming to this committee. Thank you for presenting your frank and forthright information. You can leave now, but we still want to discuss the motions before I adjourn.

Thank you very much for that.

I would suggest that we deal with the motions at the front of the next meeting. Also, with the consent of the committee, I would put the committee business we had to deal with today to the back of the next meeting, and then we then we can discuss it at that point, if that's okay.

The meeting is adjourned.

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

SPEAKER'S PERMISSION

Reproduction of the proceedings of the House of Commons and its Committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the *Copyright Act*. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a Committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the *Copyright Act*.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its Committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

Also available on the Parliament of Canada Web Site at the following address: http://www.parl.gc.ca

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

PERMISSION DU PRÉSIDENT

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la *Loi sur le droit d'auteur*. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la *Loi sur le droit d'auteur*.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

Aussi disponible sur le site Web du Parlement du Canada à l'adresse suivante : http://www.parl.gc.ca