HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Procedure and House Affairs

PROC • NUMBER 028 • 1st SESSION • 41st PARLIAMENT

EVIDENCE

Thursday, March 15, 2012

Chair

Mr. Joe Preston

Standing Committee on Procedure and House Affairs

Thursday, March 15, 2012

● (1115)

[*English*]

The Chair (Mr. Joe Preston (Elgin—Middlesex—London, CPC)): We will go ahead and start our meeting.

I'd like to thank our guests for coming this morning. I apologize for the delay. We needed to move rooms so that we could televise.

We are starting our study on the order of reference regarding the motion of privilege for the member for Provencher.

I will caution our guests today and committee members that we'll start in public and do as well as we can to talk about the issues of the breach of privilege and items that relate to that. As chair, I do feel that there may be a time when we'll get to points or issues that may require us to go in camera for security reasons.

I ask members from all sides as well as the witnesses, if you feel we're getting near there, to warn us. We'll try to delay as much of that as we can until the end of the meeting so that we can bunch it all together, instead of going in camera and back into public. So we'll do that.

Members, we were also given another motion of privilege today by the Speaker, and as a committee we will need to discuss that and where it fits in our schedule. I recognize you're all using midnight to six just for sleep right now, and we can probably use some of that.

Madam Clerk, it's great to have you here today. I would like you to lead off and introduce your guests, and then we'll go into rounds of questions.

Ms. Audrey O'Brien (Clerk of the House of Commons): Great.

Good morning, Mr. Chairman. It's a pleasure to be here today.

[*Translation*]

It is a pleasure to join you to discuss this very important issue. I am accompanied by two of my department heads. Louis Bard is the Chief Information Officer of the House of Commons.

[*English*]

He is responsible for the Information Services Directorate. The Sergeant-at-Arms, Kevin Vickers, is responsible, among many other things, for security, through the security services of the House of Commons, for providing the physical security of the parliamentary precinct and of course of members.

I don't really have an opening statement as such, but I have a few opening remarks, perhaps, to situate this discussion in terms of how we view things.

I'm very pleased that you chose to invite the Sergeant-at-Arms and the CIO, because I see very important parallels in the way each of these service heads operates in order to ensure the security of the precinct.

The first thing that I want to say is the security posture here at the House of Commons is always intelligence-led. There's a parallel between the physical security that's provided through the Sergeant-at-Arms and the House of Commons security services—and their partners—and the IT security provided through the chief information officer and the House of Commons information services team.

I'll explore that a little just to give you an idea of how we approach this. Obviously I'm not an expert in security. These are the experts I rely on, and I am really very confident that the House and members are in very good hands.

Let me first of all turn to something that's perhaps less foreign or less difficult to understand. This is what the Sergeant-at-Arms does. On a daily basis, the sergeant and his director of security are in touch with our security partners—the RCMP, the Ottawa Police, CSIS, etc.—to discuss the threat-level assessment for that day, for the precinct and for members. This goes on on a regular basis. It's a regular conversation they have.

If for whatever reason there is an elevated threat level, whether it be for the precinct because of a particular demonstration that's going on related to a summit that's happening somewhere else in the world, or something like that, or whether it's, for whatever reason, an interest in a particular member or a minister, or something like that, then the outside partners who are responsible for this continuing monitoring of the threat level will tell us what they recommend as the threat-level posture. If the threat level is such that it is elevated, for whatever these reasons might be, we then adjust our posture appropriately here in order to respond to that and to be able to do our part in the seamless protection of the precinct and of members.

Obviously, no details of those kinds of adjustments are discussed publicly. The consultations are not even discussed publicly. In the interest of good security, you keep this basically quiet, and you get on with the business of protecting the precinct and members.

In a very similar way, and on a regular basis, the chief information officer and his team are in constant contact with CSE, the Communications Security Establishment, to monitor cyber-threats. One of the things we are all trying to adjust to is the fact that the Internet, for all of the wonderful access that it provides, is nonetheless something we're all coming to grips with in various ways. The new and ever-expanding use of social media means that there are all kinds of things happening out there in cyberspace. We have to be aware of what's going on there; but at the same time, we have to make our peace with the idea that we can't control it.

It used to be that demonstrations for or against a particular issue or position, or whatever, were fairly straightforward. People had placards, they gathered on Parliament Hill, on the lawn, they shouted slogans, they heard people, they applauded, and then they went home. And that was fine. Some of that still occurs, and that's fine too. But increasingly there are now organized campaigns for and against various issues, advocating positions and so forth, that take place using the Internet and using social media. Those, of course, with the usual range of human behaviour, range from the conscientious and the serious, right through to the anarchic, and the perhaps more threatening, as in the case, for example, of this Anonymous group.

● (1120)

The difficulty one has there, in a way that perhaps other organizations don't entirely face—I'm thinking of businesses and the like—is that when we create a parliamentary network here, the campus network for information technology, it is built to what we believe is an appropriate security level and we monitor that constantly. But the important thing to remember is that from our point of view—and I believe from the point of view of members, since the network exists to serve members in the first instance—it has to be accessible to people who want to reach you. The communication going both ways, from here out and from out in, is the bedrock of political conversation in this country. We can't protect a situation to such an extent that access becomes so cumbersome and so difficult as to become an irritant, or worse yet, God forbid, an obstruction to this free flow of information and communication.

At the same time, I think we have to realize that regardless of how one might want to create a network, a situation that is hacker-proof is simply not possible. The WikiLeaks business that happened, which garnered headlines some months ago, is a perfect indication of that. There really is no such thing as a perfect network. If you say that, you issue a challenge, and somewhere out there there will be somebody who is bound and determined to break in just basically because that's how they pass their time. I think we have to make our peace with that.

What we have to do—and this is something I'm confident we are doing—is take very seriously the idea that we need a protected network, that we need a secure network, in order for parliamentarians to do their work. We do that by monitoring very carefully the activity on the network on an ongoing basis so that anything that seems unusual is something that immediately jumps out. We do that in various ways through the security measures that are in place. When we see some kind of unusual activity, we take appropriate action to address that activity, whether it's isolating a particular computer or whatever. All of this of course goes on with our partners at CSE and the stakeholders there.

We have various ways—and I won't get into the details of them, not least of all because I don't think I could explain them adequately—and various themes, I think, under which our operations fall. There is the idea, for instance, of protection. We have firewalls around the parliamentary network. We have filtering gateways. We have encryption software. In terms of detecting unusual activity, we have the usual types of software, the anti-spam and anti-virus software that's out there, which is constantly being upgraded and monitored as systems and technology develop.

Access control is certainly very important. I remember testifying before you on a different case in which we said that a network is only as secure at the weakest person using it. So whoever is using it,

[*Translation*]

It is very important to know who has access, who has the passwords and all of that. There are very important protocols that govern the use of the network.

The other aspect is the physical security of the different pieces of equipment we have, naturally.

[*English*]

So that's the physical security, whether it be laptops or whatever.

In communications between the network here and the network in your constituencies, that is possible through the creation of what's called a VPN, or a virtual private network. It allows for secure communication within the network environment.

Administratively, we have awareness campaigns in security that are run by the Sergeant-at-Arms and the CIO. We have appropriate policies, from the wearing of badges to the appropriate use of technology.

We try to sensitize people to the dangers out there, without overreacting in such a way as to give more attention than is merited to various troublemakers who ask for nothing more than a chance to make headlines.

We work very closely with CSE and with CSIS. I have here an extract, a statement from CSIS, which I think is useful. It says:

> The threat of attacks on critical information systems and the infrastructures that depend on them will, in the foreseeable future, be almost impossible to eliminate entirely, owing to the fact that attack tools, networks and network control systems are constantly evolving. As new technologies develop, so too will new attack tools along with the sophistication of the perpetrators who use them.

I don't want to leave the impression that the situation the Minister of Public Security suffered was anything that we condone. It was nothing short of appalling. But at the same time, I think we have to put that in the context of what is happening in the world today. It should not engender unwarranted anxiety about the thoroughness of our security posture.

● (1125)

[*Translation*]

That's about all I had to say.

[*English*]

We're in your hands for answering questions, and my two experts are of course at your disposal.

The Chair: Thank you, and thank you for bringing your experts.

We'll go to Mr. Lukiwski.

Mr. Tom Lukiwski (Regina—Lumsden—Lake Centre, CPC): Thank you, Chair.

My thanks to Madam O'Brien, Monsieur Bard, and Mr. Vickers for being here.

What most of us will be concentrating on, I think, is information you can provide on cyber-threats to the computer side of things. We're going to be talking to some law enforcement agencies over the course of the next few meetings to assess the threat Anonymous might pose beyond the precinct here in Parliament. So most of my comments will be directed to Monsieur Bard, although I would invite commentary from all of you.

Thank you, Madam O'Brien, for answering some of the questions I had in your opening statements.

First, given that no one can put security protocols or provisions in place that would render a system completely bullet-proof, I'd like to know right now, in your considered opinion, how vulnerable are we? How vulnerable are we if Anonymous wants to hack in? Secondly, do you have any plans to increase security provisions beyond what we currently have in the parliamentary precinct? Lastly, would you have any recommendations for our systems beyond the parliamentary precinct? I'm thinking specifically about our constituency offices.

One at a time, please, give us your assessment of how vulnerable we are right now, and then tell us what security provisions might be put in place.

Ms. Audrey O'Brien: Before I ask CIO Louis Bard to reply to Mr. Lukiwski's question, I want to say that the threats from the group Anonymous really had nothing to do with the network. This was something posted on YouTube, so it's completely outside our control or our environment.

With regard to the hacking situation and what measures are in place, Louis can speak to this matter.

Mr. Louis Bard (Chief Information Officer, House of Commons): Thank you.

Those are very good questions. There's no doubt that the House of Commons as a symbol of Parliament is regularly identified in potential security threats. Every threat you can find out there, Parliament is noted somewhere because of the symbol of Parliament.

We are, as mentioned by Madam O'Brien, working very closely with all kinds of partners, such as CSE. We're working with RCMP. We are working also with the industry. We've highlighted a number of scenarios, technologies, and layers that we have to protect the environment, and we rely on the industry in terms of also bringing a third dimension to the threats, what's going on, and what we should be preparing ourselves for. Therefore, as Kevin does on physical security, every day we assess those threats, every day we evaluate the situation.

Around three or four years ago the board approved the creation of an IT security team, which we have implemented. We have put in place a lot of new technologies and mechanisms to secure the environment.

For us, when something happens like it did two or three weeks ago, there's no doubt that at that point we strengthen our monitoring activities based on the threats. We have a lot of alarms. We follow up on alarms. We follow up on notices. We make sure that we reinforce our security measures. We make sure that we make adjustments to our protocols of the day. A good example of that is the major spoofing that happened to the Treasury Board last year. Immediately, we were ahead of the game to analyze this, and there was actually no incident to Parliament Hill following that incident.

We also adjusted our BCM strategies, such as how to deal with international threats, as an example. If need be, I can export my website somewhere else to protect the campus. There are all kinds of strategies behind the scenes that are possible, and we can act very rapidly. There's no doubt we always maintain a very close meeting with our other officials, with CSE and others, to make sure we can inspire ourselves on everything that is possible to minimize the impact.

The bottom line for me, however, is the way we make decisions. My job is to provide access to services to all members of Parliament, to provide transparency, and to make sure I eliminate all those stresses. We reject 70%, I would say, of all e-mails sent to Parliament before they enter Parliament Hill. And beyond that, we provide members with tools to identify spam, to try to filter that, and to put rules in place. At the end of the day, I still believe I need to leave the members with the flexibility that they need to operate.

Concerning the riding offices, there's no doubt that in Ottawa it's a secure environment. It's well protected. We provide all kinds of tools to members in their ridings. However, in your ridings, you've made the decision. You've set up your environment and how you want to work. Therefore, I can only be there to help, to advise, to suggest that you use a secure tool we provide you with. I have not a lot of control when you are in your constituency, but we always remain available to help you this way.

In term of the recommendation, there's no doubt that the acceptable use policy gives you a good framework in the ways you operate. There's no doubt about it in terms of how to better use the IT resource on Parliament Hill. But the same things can apply with your staff in your riding and how you behave yourself in your riding. They're good guidelines. At the same time, as we always say, it's so essential to separate your job as a member from your personal life. Very often we try as much to keep that totally separate—how you set up your house, your families, how you decide to create other Internet access, having your own private e-mail accessibilities, outside of the environment of the House of Commons. It's also a strong recommendation. It's exactly what I do for myself.

● (1130)

However, security is evolving every day. It's a question of every day we need to make.... It's like peeling an onion. There's always something new to discover. The strength that we have is the ability to react. I think we have proved that several times. And there's the board has supported us and this committee on all of the investments we've made in security technology over the last ten years.

● (1135)

The Chair: Thank you. You are well past.

Madam Charlton, for seven minutes.

Ms. Chris Charlton (Hamilton Mountain, NDP): Thank you very much, Chair.

Thank you so much for your presentation this morning.

I want to start at perhaps a more general level. As you know, when the Speaker makes a prima facie finding of privilege, that is what is referred to our committee. We have three responsibilities in that regard. Our first one, of course, is to confirm whether there is in fact a finding of privilege. And then it's incumbent on us to identify the culprit. Then our third task is to explore possible remedies to the breach.

I'm looking for some guidance here. It seems to me, although I don't want to prejudge the work of the committee, that all of us feel very strongly about the principle that all of us need to be free from threats or any kinds of attempts to intimidate us in our work as members of Parliament. I think we will likely be able to come to agreement on that fairly quickly.

It's not as clear to me how we go about identifying a culprit in this case. I recognize that this is also not unusual, and that in lots of other points of privilege we've been in that situation where culprits haven't in fact been identified. But I wonder whether you could give us some guidance in terms of how you think we ought to be framing our investigation here as committee members to actually take our responsibility with respect to the second and third referrals to us seriously, and how to do our work effectively, both with respect to identifying the culprit and then, in that context, how we pursue remedies.

Ms. Audrey O'Brien: Thank you.

The question that you ask really goes to the heart of the work of the committee on this issue. It's certainly not an easy task, partly because, as Ms. Charlton has said, this is an unprecedented situation, in that the attacks in question come from an unknown entity. The name Anonymous is there. As I understand it, that particular title or brand is out there; the various loose grouping of people who operate under its banner encourage the use of that title for people who are protesting in various ways.

If I may be very blunt, I don't see much to be gained by trying to identify the culprit as such. I think that this exercise—and in this sense I'm very happy that this isn't an in camera meeting and that we can talk this way—is a very useful educational opportunity for everyone to realize that for all of the advantages and for all of the extraordinary.... I remember reading somewhere somebody comparing the Internet to having at your disposal the library at Alexandria.

For all that this is the case, there's also a sort of darker side to it, an ability for people who want to make mischief or who want in fact to engage in activities, as the Anonymous group do in the threats they have uttered.... That's also a possibility there.

The Sergeant-at-Arms and I were discussing this question this morning when the three of us were meeting prior to coming before you, and he was reminding me that it's a criminal offence to threaten a public official. One can assume that the Minister of Public Security has talked to the authorities with regard to whatever appropriate inquiry is to be made at a policing level.

With regard to this committee, frankly I'm not sure that seeking out a culprit as such wouldn't be a giant waste of time, because I think that the nature of these attacks, as I understand it and from the reading that I've done, is that they're extremely fluid. It is not even that you have—as you might have, for example in the Wikileaks situation, wherein you have Julian Assange saying he's the head of this and wherein he has taken ownership of a particular approach to information and so forth.... This is really a set of people whose way of protesting, I gather, is basically to cause difficulties for various institutions. It has a whole anarchic side that is very dark indeed.

At the same time, I think that what is important for this committee to recognize and to applaud is the many ways in which informed citizens are using the Internet and using social media to have conversations about political issues and to take sides and to advocate in one way or another. The engagement—and the engagement over space and time—that the Internet permits is something that is to be applauded. We shouldn't let the people who want to use this for evil, for lack of a less simplistic way of putting it, carry the day. That's one thing.

In terms of remedies, I think really awareness is the most important thing, awareness that if you're using Wi-Fi in a cafe somewhere and are on the Internet, you're more likely to be open to attacks than if you're just sort of looking at new sites and so forth.

I don't know that this answers your question fully, but that would be my take on it.

● (1140)

Ms. Chris Charlton: Respectfully, with regard to remedies, this isn't about the minister having used Wi-Fi in an inappropriate way. This was an uploading of a YouTube video that would have happened regardless of whether any of us use Wi-Fi.

Ms. Audrey O'Brien: Oh, absolutely. I guess I was linking this to the hacker conversation earlier.

Ms. Chris Charlton: As I said, I feel really strongly about being able to do my work free from threats and intimidation, but I also feel equally strongly about freedom of speech. As you suggested, there's a vibrant conversation to be had.

So with respect to remedies, I don't think it is so much saying to us "don't go into Internet cafés". I think if the remedies exist, they are in an entirely different direction.

I don't think I have any time left, and I regret that. Perhaps we can continue this—

Ms. Audrey O'Brien: Forgive me. I think I may have gone on too long, which is a tendency of mine.

You are absolutely right, and I didn't mean to trivialize this as a matter of staying away from Wi-Fi. But as soon as you look at the possibility of limiting what goes up on YouTube, you get into a conversation about freedom of speech. That's a whole thing that I leave to you to sort out.

The Chair: Thank you.

Thank you, Ms. Charlton.

Monsieur Garneau, you have seven minutes.

[*Translation*]

Mr. Marc Garneau (Westmount—Ville-Marie, Lib.): Thank you, Mr. Chair.

I would also like to thank the guests who are with us today.

In short, the Speaker recognized that there was, on the surface, a question of privilege. I am certainly not calling into question the decision that was made. It led to the following motion:

> That the matter of threats to, interference with, and attempted intimidation of, the honourable Member for Provencher be referred to the Standing Committee on Procedure and House Affairs.

Frankly, I have been scratching my head since March 6, since the decision. I most certainly respect it. When I spoke, I said that it was important for the RCMP to be involved immediately because there had clearly been a threat. We all recognize that it is criminal and despicable. I've been wondering what else we can do.

You may have summarized the situation well by saying that being threatened from time to time is inherent to our profession. The Prime Minister, for example, is always physically surrounded for his protection.

[*English*]

We also know that on occasion ministers have had to be provided with protection because of a particular bill. It's in the nature of our business, and I believe I tried to make that point when I intervened before the decision was made. It goes with the job, in a sense, and it's something that we, and particularly cabinet ministers who bring forward laws, have to be aware of and accept.

So what can we do in these circumstances? You suggested awareness that these things can happen to us, and protecting access to our Internet materials, and that kind of thing.

By the way, I was hacked yesterday on my Twitter account. I must have been tired, but I was pulled in by probably a very old trick and realized that people are out there doing this kind of thing. That is something we should be more aware of; there's no question about it.

It seems to me that you are also saying we can react to individual cases and see what we can do and what the appropriate measures are. But at the same time, to some extent this goes with the job; while we want to protect members of Parliament as much as possible, we cannot provide a magic bullet here.

If Anonymous, for some miraculous reason—and I doubt that this will be the occasion—were to be caught and disbanded, there will be others. There are the OpenMedias and the Leadnows that make you aware that they are not in agreement with what a government decides, but they do so democratically; then there are the Anonymouses. But there will be lots of them, and that's the 21st century.

So what can we do—I'm asking the same question everybody else has asked—other than educate ourselves and be very careful?

● (1145)

[*Translation*]

Ms. Audrey O'Brien: Mr. Chair, Mr. Garneau's description of the situation is, in my opinion, very appropriate.

[*English*]

You were speaking about being hacked on your Twitter account. The important thing to know is that because you are on Twitter you are outside any kind of protective network, so basically anything goes. That's the whole other side of the social media thing.

[*Translation*]

Regarding the question of privilege referred to the committee, based on my understanding of what was said, everyone, no matter the political party, agrees that by issuing these threats, the Anonymous crossed certain lines. As members, you lead a public life, and in these conditions, you are ready to have your political positions attacked, but threats against a person are unacceptable. I know this statement may seem to lead to nothing, but it is important, in my opinion, that everyone unite to say that

[*English*]

there are lines that ought not to be crossed.

The Chair: Monsieur Hawn, take four minutes, please.

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

Thank you all for being here.

Mr. Bard, I just want to clarify this. You said that 70% of the e-mails that approach the House of Commons never get to our computers. Well, first of all, thank you. I appreciate this.

Some hon. members: Oh, oh!

Hon. Laurie Hawn: That's an astounding number. Is it all spam? What are those?

Mr. Louis Bard: It could be spam. There are a lot of rules. The e-mail has to be valid, it has to be addressed properly, it has to have a proper sender. You cannot send an e-mail just to "Parliament"; it has to be addressed to a member of Parliament. Also, you cannot replace who the sender is. It cannot be a group sending.

We have a long list of rules that over the years, following industry best practices, we have applied to make sure we do not corrupt or fill your mailbox with unwanted e-mails that have no meaning.

Hon. Laurie Hawn: That's excellent.

We could all ask the same question, to editorialize a bit. Everybody supports free speech. Whether I agree with the person or not, I appreciate somebody's courage in being willing to speak up about whatever and identify himself or herself. I think it's safe to say that Anonymous is a coward. I have nothing but contempt for anybody or any organization that abuses free speech in this way.

Clearly, extortion is a crime, and I hope that the RCMP and whoever else.... As Marc said, they're like the Taliban: we'll never run out of them; they're always going to be there. But I think we should take any chance we get to track one down and make an example, and I hope they are proceeding with that.

Mr. Bard, we talked about the constituency set-ups, and you have advice. Is there anything to be gained by imposing on your good offices if anybody wants to have somebody come to assess what is happening in a constituency office by way of protection? I realize that there are 308 of us and that this might be a little onerous, but is this something we should be looking at?

● (1150)

Mr. Louis Bard: Yes. We offer that service—not sending somebody to your local office, but we can arrange to provide consultation and work with your office and advise you accordingly.

Hon. Laurie Hawn: At the risk of putting words in your mouth, would that be a pretty good idea for all 308 of us to do, if we haven't done it?

Mr. Louis Bard: Well, it's really the member's privilege to ask for this. I will advise that if you have not developed for your office this kind of plan, business continuity strategies, how do you secure your environment? How do you allow your volunteers to work on your network? How do you know it's the right person you're calling on a conference call? There's so much that is under your control.

I always say that my best clients are the members and my biggest risks are the members and their staff and the employees of the House.

Hon. Laurie Hawn: Yes, you bet.

Here is a technical question, going back to Anonymous and YouTube. YouTube can technically identify who put those videos on the site. Is that a true statement or not?

Mr. Louis Bard: I think this is the difficulty, because those who act as "Anonymous" are very creative. You can receive something from China that was issued here in Ottawa. They specialize in scanning the environment and identifying weaknesses and vulnerabilities of technologies; that's what they do. Very often they get their dirty work done by others. They will give the open door, the possibility to post something to activate a script.

This is a very complex situation. We've seen cases in the States in which they worked for more than two years and finally identified five of them. But it took two years to find them, and this group is in constant mutation. Every day, it's a difficult task. It's beyond the boundaries of Canada; it's worldwide.

Hon. Laurie Hawn: Yes, and not to get into methodologies, would organizations like CSEC have the capacity to follow those chains back, whether it comes through China or wherever? Do we have the technical capacity to do that?

Mr. Louis Bard: Yes.

The Chair: I'm sorry, but your time is complete.

Mr. Comartin.

Mr. Joe Comartin (Windsor—Tecumseh, NDP): Thank you, Mr. Chair.

Thank you, witnesses, for being here.

I want to pursue the issue of identifying the culprit in terms of what our staff.... This may be for Mr. Vickers, or perhaps Mr. Bard, but I think it's more likely for Mr. Vickers. Clearly there has been some success in the last couple of years, both in England and in the United States, one as recently as about a week ago in the United States, where Anonymous or other individuals—I don't think you can call them a group—hiding behind that have been identified and are being prosecuted. I don't know if there are going to be convictions, but I have here a series of incidents where there have been charges laid in the last year or two years.

Do we have—does the House have—a relationship with our police forces? In a situation like we have here with the member for Provencher, where we would be having contact, is there a protocol whereby we would be having contact to make sure this incident was being investigated by our police forces? Also, given the most recent one that the FBI identified in the United States, were they checking to see if our police forces have been in touch with them in order to see if there are any resources they can provide us to try to identify the culprit and have the person charged?

Ms. Audrey O'Brien: Mr. Chair, I'll turn it over to the sergeant, who obviously knows more about the consultations among police forces. I think we have a very good working relationship with the authorities and we use that. At the same time, I think that the House as an institution, we as the House administration, do not seek investigation on a particular case.

Kevin can perhaps speak to how police would react and what would start them on an investigation.

● (1155)

Mr. Kevin Vickers (Sergeant-at-Arms of the House of Commons): Generally, Mr. Comartin, it's our practice to be in contact with our security partners on a daily basis. Obviously, as Sergeant-at-Arms I'm responsible for all your security, so if anything comes to our attention, regardless of what it is, we always take the appropriate steps to ensure that the proper follow-up is being taken. That would be in this case as well.

Mr. Joe Comartin: So in the situation with the public safety minister, is there a formal complaint lodged, whether it be with the RCMP or some other police force? Has that happened in this case?

Ms. Audrey O'Brien: Mr. Chairman, the sergeant would not like to get into the details of this individual case in a public situation. I think it's fair to say, though, that the House as an administration wouldn't be in a position to make that kind of complaint—just to clarify that.

Mr. Joe Comartin: Okay.

At a more general level, Mr. Vickers, you're indicating regular contact with other police forces. Again, Mr. Bard may know this. For these incidents where charges have been laid, in both England and the United States, would our staff be monitoring those charges to see what the outcome was?

Mr. Kevin Vickers: It would be my practice if I were aware of a certain threat against any member of Parliament to ensure that proper follow-up was being taken with that particular member of Parliament. I and our staff would keep ourselves apprised until the matter was resolved one way or the other.

Ms. Audrey O'Brien: If I may, Mr. Chair, I think it would be overstating it to say that we would monitor the outcome of the investigation in the United States or the United Kingdom. But we'd certainly keep ourselves aware of the developments there.

Mr. Joe Comartin: Just in terms of I guess the public generally, would we have the right to expect that for the most recent case in the United States, which I think has been seen as a fairly major breakthrough in terms of their ability to track—that was specifically Anonymous—they would be monitoring that?

I'm sorry, maybe I should explain what I'm looking for here. One of our responsibilities is to try to identify the culprit. I'm looking for sources that may be able to give this committee some assistance in that regard, recognizing, Ms. O'Brien, what you've said.

There's no way this committee has the ability to identify the culprit. It's going to have to be done by someone else. So I'm trying to figure out if that assistance is available either through our police forces or through our police forces having contact with police forces in other countries.

Ms. Audrey O'Brien: I think maybe the sergeant can answer that.

Mr. Kevin Vickers: Mr. Chair, I can assure you that we, the House, are in contact on general practices and procedures. In the case in particular with Anonymous, I'm aware of recent successes you're referring to.

I'm also aware that the Royal Canadian Mounted Police are considered world-class on these types of investigations. They work hand in hand with the other security partners around the world in doing those. It may benefit the committee at some point in time to have those RCMP experts come before you to give you pertinent information.

The competencies, as far as I know, are certainly there. As you pointed out, there certainly have been a number of recent examples where success has been obtained in identifying, through criminal investigation, who is responsible.

The Chair: Thank you.

Thank you, Mr. Comartin. I allowed you to go very long because the chair was very interested in the answers too.

Mr. Albrecht, keep it as interesting, will you, please?

Mr. Harold Albrecht (Kitchener—Conestoga, CPC): Oh, Mr. Chair, I'm not sure I can guarantee that, having worked with Mr. Comartin.

Thank you, Mr. Chair, and thank you to our witnesses for being here.

As I try to review this and get a handle on it, it seems to me there are three levels of concern. One is the parliamentary precinct.

Mr. Bard, thank you for assuring us that many of the e-mails that would arrive here don't arrive, as they would simply be problematic.

The second layer is the constituency office. As I recall, when we set up our constituency office we received a very good package of material, with good information, good instruction. In fact, I think there were some pretty clearly proscribed practices we were not allowed to engage in. I think that's healthy.

I have a concern now, after hearing you today: is that being monitored on an ongoing basis, or should I be proactive, as an individual member of Parliament, in asking for help in my constituency office to be sure that it's on an ongoing basis, and as safe as it was when we started?

My third question—I'll get them all out, and you can maybe touch on all of them—has to do with another area of concern that I think all of us around the table would share. What about our personal computers? What about our families' computers? What about our staff members' personal computers? Are there things we should be aware of in terms of preventive measures that we should be taking as individuals? And if in fact that is true, are you available for counsel for us on those issues as well?

Voices: Oh, oh!

Mr. Harold Albrecht: Now I've crossed the line.

● (1200)

Mr. Louis Bard: That's a very, very expensive question.

Voices: Oh, oh!

Mr. Louis Bard: No, no, there's no doubt that we always work really hard on our awareness campaigns for the members, providing you with information kits, documents, doing your inventory, assessing your computers. We have laptop clinics. When you come back from a summer recess, we watch in the chambers to make sure that there are no surprises you're bringing back for us on your laptop from your riding. We try to be ahead of the game and to be able to help you as much as we can.

However, you are the person running the constituency office, so you need to have those best practices to redo your risk assessment, to have a package that you review regularly to make sure that you understand your risk and understand the issues and if there are any threats or anything like this. And yes, we can always refresh that and help you with that.

The same kind of exercise can be applied to your family. You can use the same material to apply security within your own house, because the same questions will apply on how you set it up. Do you have good protection? Do you maintain your antivirus? There are so many things you can do. How do you do your banking, and who has access to what?

Mr. Harold Albrecht: I do appreciate the offer that your department makes, each time we come back from our constituencies, to look at our laptops. I've always taken advantage of that, and I think that's very helpful.

Is there a process similar to this that would sort of prod or nudge our constituency office staff to be sure that they're also engaging in a similar repetitive review process to be sure that...? Or do we have to be proactive on that as individual MPs?

Mr. Louis Bard: If members are interested, I think we can give you a package that can be used to assess your own situation. We can find ways to review this on a regular basis to make sure that we prompt you to look at this.

Mr. Harold Albrecht: I don't know how frequently that would happen, but if on a "regular basis" we would get updates and recommendations from your office and possibly an offer to even remotely review what we're doing and what we're not doing, I would find that helpful.

Thank you, Mr. Chair.

The Chair: Thank you very much.

Mr. Lukiwski.

Mr. Tom Lukiwski: Thank you.

I just want to go back for a moment to the vulnerability issue. I appreciate all that you do and continue to do while we're in the parliamentary precinct, but my question is what happens when we leave the precinct? Obviously cabinet ministers travel extensively on an international basis, but individual members also do. We have parliamentary associations that are constantly going abroad. How vulnerable are members when they're outside the precinct? We still have to be in contact. In the case of cabinet ministers, there's a lot of parliamentary work that goes on whether they're in Ottawa or in China or some other location. How vulnerable are those members who are travelling internationally?

Mr. Louis Bard: I think there's a high level of vulnerability, especially if you travel to foreign countries, because they probably know you are coming and somehow they will be watching you or observing who is out there and will follow you through the process. This is where your choice of technologies and what you use when you're travelling is so critical. As an example, if you are bringing confidential documents, secret documents, on your laptop, you are very vulnerable if you lose that laptop, if you have not secured the documents, encrypted the documents, encoded the documents, waterproofed the documents: there are so many things you can do to secure a document. At the same time, I will not bring secret documents while I'm travelling. I will find other ways to move these documents around.

● (1205)

Mr. Tom Lukiwski: Are there any specific protocols you would suggest for those members who may be travelling internationally, or are they just vulnerable no matter what they do? A lot of this is common sense, and we understand that. But are there any specific protocols or provisions that you might suggest or that you're looking into based on the fact that we may be targeted by Anonymous or other groups now?

Mr. Louis Bard: I will give the same comments I gave last year when we were looking at developing committee reports. Often the problem with security is that people don't assess what they intend to do while they're travelling. You should really assess those risks before you travel, and then we can put in place proper measures to help you during your travel through some specific packages, specific tools, or specific telephones or BlackBerrys. There are all kinds of things we can do to help you: don't use your cellular phone, use a land line.... As a preventive measure, before you go we need to understand the purpose of the trip and what you intend to do, and from there, based on the risk, we can really identify the solutions.

The Chair: You have a minute left.

Mr. Tom Lukiwski: Thank you very much.

Is there any history of any member's computer system being hacked? If so, what process do you follow there?

Mr. Louis Bard: We follow the same thing as the IT acceptable use policies on a regular basis.

It's happened at the caucus level, on your caucus web server. We've helped many of you with your caucus servers when there has been infiltration, corruption, spam, and things like that. This has happened with members' laptops that have been infected with viruses.

When we detect something, the first thing we do is inform the member and then request permission to remove that PC or that laptop to help restore the situation very rapidly. We do this on an individual private basis with every member of Parliament. If we notice a situation, we try to find a compromise and identify the threats. If I cannot at one point solve the issue with the member, I will go to the whip. That's the protocol.

There have been a lot of instances over the last 19 years I've been here, but I have to say that each time we've been able to correct the situation to the member's satisfaction. Never in the last 19 years have we lost access to our network, been paralyzed for days, or had to shut down the network. Touch wood—we have been able to keep things running.

The Chair: Thank you.

Now to Madame Charlton. And I understand you're sharing your time with Madame Latendresse.

[*Translation*]

Ms. Alexandrine Latendresse (Louis-Saint-Laurent, NDP): Thank you, Mr. Chair.

First of all, thank you for the very useful information.

I have a question specifically for Ms. O'Brien about breaches of privilege, as was the case here.

I read in your excellent document that in a case in which—and this has happened in the past—it is recognized that there was a breach of privilege, but there's no way of identifying the source, nothing more can be done. A breach of privilege is recognized, and that's all.

In this case, it is quite clear that there was a breach of privilege, given that the minister received threats specifically related to his work. In fact, he was being asked to withdraw the bill. That being said, I think that Anonymous, as was said earlier, is something intangible. We can't even say it is an organization, because anyone can claim to be Anonymous and put that label on their actions. It is not an organized group taking concerted actions or something like that.

In this case, are we not in a situation where, because we won't be able to find the source, it will be impossible to take action?

● (1210)

Ms. Audrey O'Brien: Mr. Chair, I think Ms. Latendresse is entirely correct. I can't see how you could identify a person or persons responsible for the threats against the minister.

As you say so well, because it is not even an organized group, anyone can use the name Anonymous, which is even encouraged by the people marketing it. In my opinion, there isn't much we can do about that.

However, I am dedicated to the institution of Parliament. Based on this morning's discussion, everyone seems to believe, as I was saying earlier to Mr. Garneau, that a line was crossed by Anonymous. Threats were used, which is unacceptable.

One of the things I learned this morning is that the group apparently sponsors certain malicious websites. If you oppose a bill, you are given instructions to express your opposition. In fact, they don't really help you send an email to the minister to express your disagreement; instead, they have you send something else that, suddenly, triggers a malicious process. Some people who are opposed to a bill, who may be of good faith and who would like to voice their opposition, may unfortunately find themselves on such sites.

I will say again that there needs to be education. It would be important for a report by the committee to indicate to citizens that we want them to be engaged and to participate in the political debate, but that they mustn't be fooled by things they may not understand. You have to be careful. Signing petitions and sending emails is fine. However, it is not always that simple.

I would like to clarify the following point. Mr. Bard said that 70% of emails are not sent to parliamentarians. It is important to specify what an email campaign is; they are done in certain ridings or regions and are perfectly legitimate. I'm talking about emails that have an address: that is acceptable. However, when an address is not identifiable, we have a case that is part of the 70%. I wouldn't want people to think that many emails on a given subject will not arrive because someone decided to clean up.

Ms. Alexandrine Latendresse: In fact, all members receive a lot of these emails, which are legitimate.

● (1215)

Ms. Audrey O'Brien: Absolutely.

Ms. Alexandrine Latendresse: Thank you.

[*English*]

The Chair: Thank you.

Mr. Zimmer.

Mr. Bob Zimmer (Prince George—Peace River, CPC): Thank you, Chair.

Thank you for coming today. I appreciate your being here.

For the public's benefit, I think there are really two issues here: cyber-bullying, as I call it, and security.

I'll talk specifically about the cyber-bullying. I think there's a perception in the public that to some extent we politicians are unaccessible. I certainly have a Twitter account. I have a Facebook account. I think there is a perception, especially with Anonymous—and I haven't had a dialogue with Anonymous before—that it appears that things are escalating. I guess I would challenge the public and say: "Dialogue with us. We're approachable. Start off with a dialogue, as opposed to jumping to that higher level immediately." I just would challenge them to do that.

I have a question about security, though. We're Canadians and we have good security systems as well, but do we consult with other entities—the CIA, the FBI, and Scotland Yard—to see what they're doing? Do we have that interaction?

Ms. Audrey O'Brien: I'll turn it over to the CIO in a moment, but first of all let me say that I couldn't agree with you more. The idea of entering into a conversation and a dialogue with our political representatives, whether it be for or against a particular measure, is one that I think is entirely laudable.

Mr. Hawn I think said it very well about the people who engage in this kind of threatening situation, like Anonymous: it's a cowardly thing to do.

Mr. Bob Zimmer: Right.

Ms. Audrey O'Brien: It has nothing to do with real political engagement.

With regard to the cyber-bullying and the question of security, I mentioned earlier that CSE, the Communications Security Establishment, is basically the authority here in Canada that is set up to look specifically at cyberthreats. They obviously have a network internationally with the Americans and with the United Kingdom.

We are, through our contact specifically with CSE, privy to the kinds of best practices that are being developed, and really all around the world, because I think every parliament is wrestling with this business of accessibility and openness versus the kind of bad situation that's faced with groups like Anonymous.

Perhaps, Louis, you have something to add.

Mr. Louis Bard: As indicated in what Madame O'Brien is saying, there is no doubt that CSE is the prime vehicle we are working with, because of their role. CSE has been very good in helping us in the choice of technologies, how to do monitoring, and all of that, and also they give us a heads-up on things that are happening. There's the RCMP, and also other vehicles within the federal government, such as ITSB and all of the shared services and all of those elements, that are good.

At the same time, my main focus is more on the tools, on the means and things like that, and we deal with all kinds of industries around the world to understand what's going on. Also, we have been visiting other parliaments and other institutions. As well, I went with Mr. Vickers to visit some security organizations in the States to also understand what they are doing. We're doing everything we can. Every piece of information and literature that we can put our hands on is part of what we do every day.

Mr. Bob Zimmer: Thanks.

I have one last question from a colleague. We're curious to know if it is possible for a particular hacker to put something onto a computer. Is that possible? It could be a false piece of information or a false document or something like that. I guess it would be similar to a virus. Is it possible to do that?

Mr. Louis Bard: There is no doubt that through attachments and through all kinds of things everything is possible. We have identified some very complex infection structures. As an example, they will connect to your PC and will try to make other connections, or import other material, or copy what is on your desktop. We've seen all kinds of shapes and forms of this and that. In every instance, we've been the first ones detecting this on Parliament Hill and have been able to inform our peers.

What I'm trying to be careful about is not to become a fishing expedition for other partners; that is not my job here. But yes, there are all kinds of possibilities. I can guarantee you that we are doing very extensive monitoring. When we see anomalies, we are very, very quick to call the members of Parliament. In each instance, I would say that members have been 99.9% very cooperative. Members, ministers' offices, whips' offices, caucuses, and caucus research—everybody is very, very cooperative.

The Chair: Thank you.

Mr. Bob Zimmer: Do I have more time?

The Chair: No, you do not.

Mr. Bob Zimmer: Thanks.

● (1220)

The Chair: Thank you.

Mr. Kerr.

Mr. Greg Kerr (West Nova, CPC): Thank you, Mr. Chair.

Thank you very much for being here. There's quite a learning curve this morning.

A lot has been covered, and your explanations are very good. Obviously we are left with questions as well as directions. Beyond what you've said, are there other things the committee should be doing as we wrap up our study?

When I hear about the things that can happen, I am wondering if it would be to our advantage to bring in some of those representatives of the private sector who develop these marvellous machines and technology so we could have a conversation with them about the kinds of things that do take place or could take place. They're outside the security issue, but they do develop the expertise that goes into it. Would that be something we should consider?

Ms. Audrey O'Brien: If I may say, Mr. Chairman, to you and to Mr. Kerr, it's up to the committee to decide where it wants to take this investigation, in terms of a learning experience as much as anything else.

Certainly one of the things Louis was pointing out is that we make it our business to have contacts with the various authorities and with private industry so that we are constantly apprised of the developments in technology as well as the flip side of that, which is the developments of the evildoers. Even as a certain type of anti-virus solution is worked out, there are hackers who will try to circumvent that, and so forth. I don't know whether you would find those discussions helpful.

Certainly I can assure you that since we're plugged into various networks, we're privy to the best practices and latest information about things that are going on, which we can use to inform our own security posture and provide better security for members and the House of Commons.

Mr. Greg Kerr: I appreciate that, but your answer didn't quite get to where I had hoped. Our job is to represent the public in the various parts of the country we come from. Obviously this is important to the public, as is what is going on beyond our security system and beyond our scope. That's why I was wondering if you'd suggest that it would be a good idea to hear from the security people, perhaps those who deal with the police and so on, as well as from the industry experts who develop it, or whether that would add to the scope of what we're looking at.

I know you've answered. I'm just wondering if that seemed like an appropriate thing for us to look at before we finished our study?

Ms. Audrey O'Brien: As I said, I think that is up to you to decide. As far as I'm personally concerned, you have the two House of Commons experts here that you need.

As for what exists out there in terms of authorities, you might find it helpful to pursue things in camera about specific situations you have lived through and so on. I'm not quite sure where the committee is taking its study.

Mr. Greg Kerr: Neither are we.

Thank you.

Ms. Audrey O'Brien: Thanks, Mr. Kerr.

The Chair: Thank you, Mr. Kerr.

Mr. Comartin, go ahead, please.

Mr. Joe Comartin: Thank you, Mr. Chair.

Mr. Bard, I'm looking right now at the e-mails that were sent to Mr. Toews from Anonymous. There's a web address on them. I'm asking about the specific case. If I came to you as a member of Parliament and asked you to trace this back to a source and then back through that to the actual source, would you be able to do that, and would you provide that as a service to members of Parliament?

Mr. Louis Bard: With regard to any request from members about e-mails they receive, if they were received on the mail system of the House of Commons, we maintain logs of e-mails and logs of Internet access. All of these logs are maintained for a certain length of time, and we are able to do some investigations.

For example, with regard to all of these videos on YouTube you referred to, there's no doubt that we've done due diligence to scan the computer environments, and I can affirm that none of those videos was posted from any computer from the House of Commons. That's very clear.

That's the extent of it. If it crosses the boundaries of the House and is outside, I don't have access to those tools.

● (1225)

Mr. Joe Comartin: Do we have a protocol in the House with CSE to ask them to do that?

Let me just say that I know from the experience I've had with the Department of Public Safety, and the work we've done in particular with child pornography sites and tracing them back to source, that at least some of this technology is available. CSE is quite frankly one of the better agencies in the world in terms of being able to do this. So do we have a protocol with them such that if you're not able to trace it back, we can ask them to trace it back?

Mr. Louis Bard: I can perhaps answer the first part of this question.

CSE does not have really any authority on Parliament Hill. However, it will cooperate, upon request, to help me manage my environment. If it's beyond monitoring or beyond managing the precinct, if it crosses the line and may be something criminal, that's beyond my boundaries, and I refer to Kevin on those matters.

Mr. Joe Comartin: Mr. Vickers, do we have a protocol with CSE in a situation where we at least suspect it's a criminal event and we want to try to trace it?

Mr. Kevin Vickers: First of all, Mr. Comartin, CSE's mandate is very, very specific. They run under very tight legislative...what they can do and what they can't do, especially if Canadian citizens are involved.

The RCMP, for example, would have competencies there and international relationships. In the case you just mentioned, for example, child pornography, they could try to drill down, if they have an IPO address, and find the source of whoever is distributing that child pornography, just as they would be distributing a video on YouTube.

So it does exist. As you referred to earlier, there are some cases of success. As the clerk has mentioned, it's a very complicated, sophisticated world they operate in, and it's getting difficult, but as you pointed out, there are examples of some success.

Ms. Audrey O'Brien: Perhaps—

Mr. Joe Comartin: I'm sorry, Ms. O'Brien; I'm going to run out of time, and I want to be clear here on where the responsibility lies.

If I believe that I've been the victim of a criminal event, am I the one who goes to the RCMP as a member of Parliament, or do we have a protocol that says it would be you, Mr. Vickers, or someone else here on the Hill? Whose responsibility is it to approach the RCMP to conduct the—

Mr. Kevin Vickers: It would be your responsibility, as the complainant, to make an official complaint with the RCMP.

Mr. Joe Comartin: Thank you.

Ms. Audrey O'Brien: Just to tie that up, when Monsieur Bard was saying that if you, for example, receive an e-mail on your Hill account, and for whatever reason you want to know where that came from, we can provide that information to you. Then, as to what you decide to do with it, if you feel that it infringes your rights such that you want to lodge a complaint with the RCMP, as Kevin says, it's up to you to do. We don't step in as an institution, in between, to make those decisions.

The Chair: All right.

That completes my speakers list. I'd be happy to take any one-off questions that anyone has.

Mr. Lukiwski, you have one? Sure.

Mr. Tom Lukiwski: This is just quick one—and excuse me, because I'm pretty much a technological Luddite when it comes to these things.

Monsieur Bard, you mentioned that 70% of e-mails are blocked coming in. Would that be to the main parliamentary number? We all have personal e-mail addresses as well. There's the office number, where most of my e-mail comes from, but we all have personal e-mail addresses as well.

If there's someone who somehow gets hold of an MP's personal e-mail address, is there any way you would be able to detect anything or block any communication in that event?

● (1230)

Mr. Louis Bard: If it's a personal address outside of the environment, if it's—

Mr. Tom Lukiwski: No, it's one of the ones we're all granted here.

Mr. Louis Bard: It could be any e-mail sent to the parl.gc.ca site. Everything sent to us will be filtered and analyzed to make sure it's a valid e-mail.

When I say “reject”, it means it's a bad e-mail; it's not a valid e-mail. It's an attempt to corrupt or deny services, an e-mail that has no real value.

If we have any doubt about that e-mail, but there's no virus or anything, it will be delivered to you, and then we'll identify the level of spam. If we believe this could be spam, it's for the members to decide what to do with that e-mail.

That's the way things work.

The Chair: Okay. I have a few more one-off questions.

Mr. Zimmer and then Mr. Garneau.

Mr. Bob Zimmer: This is more of a comment than what I said before.

This is a challenge to the public, I think, before buying into this sort of a situation where Anonymous is followed, or somehow supported. I would say the challenge to the public is.... I see it as a bigger issue. I don't just see it as a challenge to us as parliamentarians. I see it, as a Canadian, as more of a bullying issue in general. One of the comments made in the letter was,

> How does it feel to have personal information about your family in the hands of the people you know nothing about, with no control over who disseminates it or how it will be used?

I see that as a Canadian threat, as opposed to just a parliamentarian threat. I would just challenge those, before buying into this sort of all or nothing, to start a Twitter account of your own and ask these questions directly, with your name listed. I'd be happy to answer any questions, as most of us will. I think this crosses all party lines. I don't think it's a partisan issue at all. I think the dialogue is there; we're open to it, so let's have it. Okay.

The Chair: Thank you.

Monsieur Garneau, go ahead.

[*Translation*]

Mr. Marc Garneau: Thank you very much.

[*English*]

My one question I guess is based on my ignorance. Is there any gatekeeping done of any kind with respect to YouTube? Can anybody post anything and it is not monitored or checked to see whether it breaks the law in any way? Is there any discussion internationally about having those kinds of standards before something can be posted as a YouTube video? Or is it a wide-open wild west?

Mr. Louis Bard: Well, I have always been developing this environment with a concept of an open Parliament, open dialogue. As you are aware, there was a Speaker's decision two or three years ago about opening the members' permission, allowing downloading data, re-using our content.

I think your question is very valid, Mr. Zimmer. Members will have to find new ways to engage with constituents.

At the same time, because of all of that, never will I claim that I will try to analyze your e-mail, analyze what you're posting, analyze.... I'm not doing that. It has to become the members. We do not do any kind of surveillance that way.

Mr. Marc Garneau: The question was not specific to Parliament. It was just applicable to the whole planet, really. It was really more of a general nature—anybody out there, not Parliament specifically. Do you know whether checks are put in, or can anybody post anything they want?

The Chair: To YouTube specifically?

Mr. Marc Garneau: On YouTube, yes.

Mr. Louis Bard: I think the answer to this is yes.

The Chair: Yes.

Mr. Kerr and then Mr. Comartin, go ahead.

Mr. Greg Kerr: Thank you very much.

It may have been covered, but I just want to clarify. BlackBerrys are a little different in some ways from computers. Are there special precautions or things we should be aware of in using BlackBerrys?

Mr. Louis Bard: I think the BlackBerry represents the highest security available for smart phones right now on Parliament Hill. There's no doubt it has achieved a high level of security certification, and therefore they are good tools to use. They were developed in support of our corporate infrastructure, and therefore they are very well integrated to the current House environment.

Also, we have allowed a very limited number of third-party applications, which also makes things quite secure. However, there are elements of the BlackBerry, like the cellular phone, the PIN-to-PIN messaging, that are totally outside the environments, and they are more exposed with this kind of environment. Therefore, again, always be conscious for which purpose you are using the equipment. It's always important. It is really a good tool to use. It protects you very well, right now.

● (1235)

Mr. Greg Kerr: Okay. Just one clarification. You were saying that PIN is less secure than the regular e-mail contact?

Mr. Louis Bard: Yes.

Mr. Greg Kerr: Thank you.

Mr. Louis Bard: Absolutely, because with PIN-to-PIN I'm talking to you; therefore, there's no network. It's just radio waves, and the security is just you and me. We're talking to each other, that's the security level. But the rest is not.

The Chair: Thank you.

Mr. Comartin, to finish this off.

Mr. Joe Comartin: This is a bit offside, Ms. O'Brien, but there's a debate going on currently, specifically because of what happened in this case, of limiting or prohibiting the access to court files in matrimonial matters. I think that's being seen in the legal community generally as a provincial responsibility because of the responsibility of the provinces to administer justice.

However, there is a federal component. If we were to amend, for instance, either the Divorce Act or the Canada Evidence Act to prohibit access to the files to the general public, I want to say I'm not in favour of that. But I'm asking whether you're aware of whether the law clerk has been asked for an opinion on that matter.

Ms. Audrey O'Brien: To my knowledge, the law clerk has not been asked for an opinion on that matter, no.

Mr. Joe Comartin: Thank you.

The Chair: Thank you.

One last little question, for Mr. Albrecht, please.

Mr. Harold Albrecht: Thank you, Mr. Chair.

Thank you, Mr. Bard, for underlining the security of the BlackBerry system. You clarified that the PIN is less secure. Is that equally true of the BlackBerry Messenger, or are those identical...?

Mr. Louis Bard: Absolutely.

Mr. Harold Albrecht: Okay. So both of those are less secure than an e-mail through our personal accounts.

Mr. Louis Bard: Yes.

Mr. Harold Albrecht: Okay. Thank you very much.

The Chair: Great.

I thank you all. And I thank you for the respectfulness of the questions today and how we didn't wander into what should not be said in public session.

Thank you very much. It was a great first start. I thank you for starting us off on this mission. As you may have heard, we're not quite sure where it's going next, but we have some other witnesses in mind, and we'll move there.

Ms. Audrey O'Brien: Mr. Chair, I understand from the Sergeant-at-Arms, in his everlasting role of monitoring the latest developments, that there was something posted on Twitter that allowed that I was doing okay testifying before this committee, but that I might be confusing “Anonymous” with a group that is “LulzSec”.

The reason I don't even try to pronounce this is because—

Ms. Chris Charlton: How come they get to ask questions?

Ms. Audrey O'Brien: Well, I don't know whether I should be apologizing to these people, or whether they're bad people I don't care about.

I think it comes back to Mr. Zimmer's point that we all have a responsibility not to be taken in by websites that are having us inadvertently spread spam or malware around.

To the Twitter person who's been disappointed in me, I will try to do better.

Thank you very much.

The Chair: I believe you were incredible, so I'll just go with that.

Ms. Audrey O'Brien: Thank you, Mr. Preston. It's always a pleasure.

The Chair: Thank you.

Anything else for the good of the committee today?

Yes, Mr. Lukiwski.

Mr. Tom Lukiwski: I was just wondering if we want to take a few minutes on committee business, since we've had another point of privilege referred to us. Plus, my understanding is that Monsieur Ménard is making a statement about wanting to come before this committee as well.

The Chair: Let's go in camera then, and we'll do committee business, with the will of the committee.

We'll suspend for a minute.

[*Proceedings continue in camera*]

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

SPEAKER'S PERMISSION

Additional copies may be obtained from: Publishing and Depository Services
Public Works and Government Services Canada
Ottawa, Ontario K1A 0S5
Telephone: 613-941-5995 or 1-800-635-7943
Fax: 613-954-5779 or 1-800-565-7757
publications@tpsgc-pwgsc.gc.ca
http://publications.gc.ca

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

On peut obtenir des copies supplémentaires en écrivant à : Les Éditions et Services de dépôt
Travaux publics et Services gouvernementaux Canada
Ottawa (Ontario) K1A 0S5
Téléphone : 613-941-5995 ou 1-800-635-7943
Télécopieur : 613-954-5779 ou 1-800-565-7757
publications@tpsgc-pwgsc.gc.ca
http://publications.gc.ca

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