HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 069 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Wednesday, September 27, 2017

Chair

Mr. Bob Zimmer

Standing Committee on Access to Information, Privacy and Ethics

Wednesday, September 27, 2017

● (1530)

[*English*]

The Chair (Mr. Bob Zimmer (Prince George—Peace River—Northern Rockies, CPC)): Good afternoon, everyone. I think we're ready to go. We have quorum.

Welcome to the Standing Committee on Access to Information, Privacy and Ethics. Today's meeting is number 69. We're studying the privacy of Canadians at airports, borders, and travelling in the United States.

I would like to welcome from the Canadian Air Transport Security Authority, John Stroud, who is the vice-president, corporate services and corporate secretary; and Natalie Sabourin, manager, information management, privacy and ATIP; from the Canada Border Services Agency, Robert Mundie, acting vice-president, corporate affairs; and Martin Bolduc, vice-president, programs branch. We'll start with Mr. Stroud for 10 minutes.

Mr. John Stroud (Vice-President, Corporate Services and Corporate Secretary, Canadian Air Transport Security Authority): Thank you very much. I'll offer some very brief remarks.

As you said, I'm from the Canadian Air Transport Security Authority, CATSA, and I'm joined by my colleague Natalie Sabourin. She's the manager responsible for privacy and ATIP. To remind you, CATSA is responsible for security at airports. We're responsible for outgoing passengers, in comparison to my colleagues who are responsible for inbound. Our mandate focuses on the screening of passengers and their baggage, also airport workers who get into the restricted area at the airport. We also offer a restricted area identity card.

In terms of privacy and the retention of information at CATSA, we have four programs in place, and I'd be happy to tell you about any of them. One is what we call our boarding pass scanning system, which scans the passenger's boarding pass when they arrive at the checkpoint. Another is CCTV cameras that we have for the checkpoint. The third is a database where we store incident information. The last is to connect with the NEXUS card.

That's an overview of the areas where we keep personal information, but we don't share information with the United States. With that brief introduction, I'd be very happy to respond to any privacy-related questions you have.

The Chair: At one minute and 41 seconds that has to be a record for the opening statement. Congratulations.

We'd like to welcome Mr. Bolduc from the Canada Border Services Agency. Go ahead for 10 minutes.

Mr. Martin Bolduc (Vice-President, Programs Branch, Canada Border Services Agency): Thank you, Mr. Chair.

On behalf of the Canada Border Services Agency, I am pleased to be here to contribute to your ongoing discussions regarding privacy at Canada's airports and borders. With me today is Robert Mundie, acting vice-president of the corporate affairs branch and the agency's chief privacy officer.

[*Translation*]

The CBSA is committed to maintaining both an individual's right to privacy and the safety and security of Canadians. Our officers are trained to conduct all border examinations with as much respect for privacy as possible.

The CBSA's information collection has always maintained a balance between protection of the border and national security, while safeguarding the privacy of the information with which we have been entrusted.

Currently, under the authority of the Customs Act and the Immigration and Refugee Protection Act, we collect routine, biographical data from the passport—name, date of birth, and citizenship—and some biometric information, such as fingerprints, in certain visa-required situations.

This information is shared with international partners when and where necessary, and is covered by legislation, international treaties, and bilateral information sharing agreements.

● (1535)

[*English*]

Collection is almost always done through automation, for instance, by scanning the machine readable zone of a passport to reduce the possibility of error. Once collected, the information can be shared systematically or on a case-by-case basis.

[*Translation*]

For example, data is routinely and systematically shared with Immigration, Refugees and Citizenship Canada, and with Statistics Canada, and can be shared on a case-by-case basis with the RCMP and CSIS pursuant to an active investigation.

Robust privacy programs and policies are in place to guide information sharing and use.

We have a statement of mutual understanding, in addition to various memoranda and information sharing agreements, with the United States, highlighting privacy principles that both parties will adhere to with respect to personal information.

We also consult regularly with the Office of the Privacy Commissioner, and have prepared detailed privacy impact analyses for various initiatives.

[*English*]

For example, the entry/exit initiative, or Bill C-21, has submitted a PIA for each phase of the project and has implemented all of the Privacy Commissioner's recommendations. We will further engage the OPC should Bill C-21 receive royal assent.

[*Translation*]

We protect personal information through restricted system access with user profiles. In addition, detailed instructions have been provided to users on how information can be shared. For instance, they must adhere to strict information retention and disposal schedules.

Individuals may submit an access to information request to the CBSA to obtain their travel history, including records of entries and, for third country nationals and permanent residents, their exit from Canada.

[*English*]

In the event of any questions or discrepancies, individuals can request that the CBSA amend or correct the information. If the CBSA agrees that information should be changed, it will also automatically and systematically inform any party who received the information of that correction.

In summary, the agency collects information to support its mandate with respect to national security, border management, and immigration program integrity. It shares information only when it's relevant, proportionate, and necessary to the administration of customs and immigration law.

Before concluding, I would like to say a few words regarding an issue that I know is of interest to the committee, the searches of electronic devices at the border.

● (1540)

[*Translation*]

As the committee is aware, courts have long upheld that travel across international borders is voluntary, and that there is a lower expectation of privacy when travelling, particularly when entering or leaving a country's borders.

The agency uses many avenues to inform the travelling public of their rights, their obligations, and what they should expect. Travellers are aware that they, and their goods, may be subject to thorough examination.

The Customs Act gives border services officers the authority to examine goods for customs-related purposes. In this context, goods are defined in section 2(1) of the act to include “any document in any form,” which therefore encompasses electronic documents.

[*English*]

The examination of digital devices and media must always be performed with a clear link to administering and enforcing CBSA-mandated program legislation that governs the cross-border movement of people and goods. Individuals also have the obligation under section 13 of the Customs Act to present and open their goods if requested to do so by an officer. Because a password may be required to open and examine documents on an electronic device, officers may compel a traveller to provide it in order to allow for the fulfillment of that traveller's obligations. The examination of electronic goods may uncover a range of customs-related offences. For example, electronic receipts may prove that goods have been deliberately undervalued or undeclared. Electronic devices may also harbour prohibited goods such as child pornography. I would like to underline, however, that CBSA policy is clear: electronic devices should not be searched as a matter of routine.

[*Translation*]

In fact, officers are instructed not to do so unless there are a number of indicators that a device may contain evidence of a contravention.

It is agency policy to turn off wireless and Internet connectivity when examining a device to ensure that the examination does not extend to material not stored directly on the device. This means that information stored remotely but accessible from mobile devices or laptops—such as social media accounts or computing clouds—cannot be searched. Officers cannot compel individuals to provide passwords for accounts that are stored remotely or online.

In conclusion, the CBSA takes its privacy protection responsibilities seriously.

[*English*]

We welcome the views of the Privacy Commissioner and we will continue to work with his office to strengthen our information-sharing activities and the way we collect, store, retain and dispose of personal information.

Thank you, Mr. Chair. We would be pleased to answer any questions from the committee.

The Chair: Thank you for your testimony.

Mr. Saini has the first round of questions for seven minutes.

Mr. Raj Saini (Kitchener Centre, Lib.): Good afternoon. Thank you very much for being here.

One of the questions I had, and I asked this of a previous witness, was on the executive order that was issued by President Trump a while ago removing the fact that privacy would not be extended to non-U.S. citizens. This question may not be clearly for CATSA, but it may be for the CBSA. What does this mean for Canadians? Can you highlight how you feel this is going to affect us?

Mr. Martin Bolduc: Well, unfortunately, it's very difficult for me to comment on U.S. policies and legislation, so I wouldn't be able to offer any comments on your question.

Mr. Raj Saini: Do we have no strategy of how we're going to deal with this at all?

Mr. Martin Bolduc: We engage with colleagues from U.S. border protection on making sure that any agreements we have in place and the rules under which we share information and how we protect it are respected. Any information that we share with the U.S. would be managed through those MOUs and treaty. As for the general passage of people at the border and what is collected by U.S. officials, I cannot offer any comments on that.

Mr. Raj Saini: When you talked about passwords, you were very clear in stating that there should be a lower expectation of privacy at the border and that, if there are certain devices you or the border officials felt could lead to some sort of finding of some information on the password device, that device had to be, I guess, demobilized in the sense that it cannot connect to the Internet, cannot go to a cloud or anywhere like that, and you cannot check any social media.

What is the reverse if a Canadian is coming through the American border? Are the rules the same, or is there a discrepancy in the rules?

Mr. Martin Bolduc: I don't know about the rules that apply on travellers entering the U.S. I'm sorry.

Mr. Raj Saini: Okay. I have no further questions then.

The Chair: You're only two minutes in, so you have five more minutes.

Mr. Raj Saini: I guess I'll go to CATSA. If people are coming to the border going outbound—this is a general question for both of you—is there some advice you can give in terms of electronic devices? How should Canadians react at the border? What should they expect? What improvements might be made? What shortcomings do you feel are there that maybe we can improve upon?

Mr. John Stroud: When you're going through the security checkpoint, you need to be sure that your device can be powered on. We're looking at it from a security point of view. We're not looking at it from a privacy point of view. We ask that the device be able to be powered on, and that's it.

Mr. Martin Bolduc: As for CBSA, I think it's important to address the myth that we often go into the personal phone of travellers. This is not the case. We conduct our examination in a progressive fashion. As we've built elements to go further in the questioning and the examination, that will eventually lead us, if we have enough grounds, to ask for a cellphone and ask the traveller to provide us with the password to be able to look into it.

The general public should not fear carrying their electronic devices across borders. As with any other electronic devices, we should be mindful of what we have on them. If we feel that there is confidential information related to business practices or you're involved in an investment and you don't want that information to be made public, or you want to keep it private, well, you shouldn't have it on your personal devices. That would be a general rule of thumb I would give to anybody.

● (1545)

The Chair: The next questions for seven minutes go to Mr. Gourde.

[*Translation*]

Mr. Jacques Gourde (Lévis—Lotbinière, CPC): Thank you, Mr. Chair.

My thanks to the witnesses for being here.

My first question is for Mr. Bolduc.

For how many years have you been checking travellers' electronic devices such as cellphones, iPhones, iTop or other devices?

Mr. Martin Bolduc: I wouldn't be able to tell you when we started doing that. I do not have that information with me.

In this day and age, the use of those devices is widespread. Really, someone who does not have a cellphone is the exception.

However, with the permission of the chair, I could check when we started using this practice at our checkpoints.

Mr. Jacques Gourde: Mr. Bolduc, do you have any statistics on the frequency of inspections? Is one person in five being inspected? Is this done randomly? If there's a reasonable doubt, I understand that you conduct an inspection, but I think it is also done randomly.

Has the frequency of inspections increased in recent years?

Mr. Martin Bolduc: I asked my team to find the mechanism that helps us gather that information. Since the public is very interested in this type of activity at the agency, I asked that we be able to keep statistics rigorously in order to make the information public.

The data I can provide is more anecdotal rather than rooted in the reality that our officers experience on a daily basis. However, the agency is committed to computing that data and making it public. I'm talking about the number of inspections of cellular or other electronic devices, and the types of devices that are checked.

Mr. Jacques Gourde: Were any Canadians surprised by this practice and did they refuse to disclose their passwords when their electronic devices were searched?

Mr. Martin Bolduc: Yes, that has happened before.

Mr. Jacques Gourde: What happens then? Do you inform the person of the regulations and demand compliance?

Mr. Martin Bolduc: It depends. We act on a case-by-case basis. In most cases, people co-operate with the authorities at the border. However, in general, an officer may order the disclosure of the password and, if the person refuses and the officer has good reason to believe that there may be prohibited material on the phone, there may be an arrest and perhaps even an appearance in court.

Mr. Jacques Gourde: Are there people who have actually filed a complaint? This is access to privacy, after all. We keep everything on our cellphones these days. It's so personal. Have there been any complaints?

In general, what are Canadians supposed to do in such a situation, when they feel wronged?

Mr. Martin Bolduc: I know the Office of the Privacy Commissioner has received complaints. I could ask my colleague Mr. Mundie to respond.

[*English*]

Mr. Robert Mundie (Acting Vice-President, Corporate Affairs Branch, Canada Border Services Agency): In the past year there have been three complaints that have come from the Office of the Privacy Commissioner, and we're in the process of co-operating with those investigations. They haven't yet concluded.

[*Translation*]

Mr. Jacques Gourde: Ms. Sabourin, do you have anything to say about the issue?

Ms. Natalie Sabourin (Manager , Information Management, Privacy and ATIP, Canadian Air Transport Security Authority): Yes. I just want to add that, in the last year, we have only received one complaint from the Office of the Commissioner related to personal information.

Mr. Jacques Gourde: If there are not many complaints, it means that people understand the importance of the search.

However, do your mechanisms have parameters to ensure that you do not take inspections too far in certain circumstances, or when you search someone, do you search everything fully, even Facebook and the bank accounts?

[*English*]

Mr. John Stroud: Personal devices, we don't search those at all. What we're looking for is a security threat. When you are going through the checkpoint, personal information on a personal device is not relevant, so we don't search for that.

● (1550)

[*Translation*]

Mr. Martin Bolduc: If I may, I'll provide a clarification.

You referred to the fact that we keep everything on our cellphones, such as our bank account information. With respect to the CBSA, as I explained in my opening remarks, we ask for the password to unlock the phone, but we put it in airplane mode. So there is no data transmission. We do not have access to people's bank accounts or other information like that; we have access to the information stored on the phone. This means that, when we search a cellphone, we do not have access to the information that people use for their bank accounts, such as a password or a bank card number. That is not part of the sort of examination that the agency conducts.

Mr. Jacques Gourde: You're talking about a cursory examination, from which it is possible to conclude that everything is fine. However, if a warning light goes off in the officer's head and he has a reasonable doubt to believe that he is dealing with a terrorist, is there a process in place enabling the officer to further search the person's cellphone, or is that the responsibility of another organization?

Mr. Martin Bolduc: Our officers do not operate on the basis of suspicion alone. They have to identify offences. If we had suspicions, we could document them, but we would not go any further in searching a telephone. We would not ask the person to activate the WiFi so that we could check other things. This information is usually obtained after an appearance in court and after a warrant is issued by a judge.

With respect to the CBSA's activities, as I mentioned, we only check what is stored on the device, without exploring any link to any network or to documents that would be stored somewhere other than on the phone. It is important to say this to the members of the committee, but also to Canadians.

Mr. Jacques Gourde: Do you feel that the number of electronic device searches you have conducted has really been worthwhile? Has something come up one time out of 1,000? Is it really worth continuing the exercise?

Mr. Martin Bolduc: If the agency believed that such examinations were not worthwhile, we would stop doing them. Unfortunately, we find child pornography and propaganda material on phones. In addition, in the case of people who said that they have not acquired anything on their trips, we find receipts on their phones that show otherwise. That examination is valid.

As I mentioned, we only do it for the purposes of the Customs Act. It is important to stress this. I would not say it is used as a last resort, but the fact is that a traveller's cellphone is not the first place we search. We start by asking questions and searching the luggage. Then, if something suggests an offence under the law, we can go so far as to search the telephone. We do not do it systematically. Unfortunately, I cannot give you statistics on that, but it is a very low percentage.

Mr. Jacques Gourde: Thank you.

[*English*]

The Chair: Next up is MP Trudel for seven minutes.

[*Translation*]

Ms. Karine Trudel (Jonquière, NDP): Thank you, Mr. Chair.

Thank you very much for your presentation.

This summer, I was talking to a friend of mine and he told me how nervous he gets when he has to go through a customs inspection. I told him that he should not, if he has nothing to feel guilty about. He is nervous by nature and, for him, it is all very official. I keep thinking about him today. So I will be smiling as I ask you questions about a very serious subject.

We have been talking a great deal about cellphone searches. Even I keep my plane tickets on my cellphone. Our phones are used for a bunch of things.

When you decide that a search like that is needed, for how long do you keep the personal information you have collected?

● (1555)

Mr. Martin Bolduc: If the information shows that an offence has been committed, there are a number of things that can be done. The goods may be seized. In case of possession of child pornography, we can arrest the person. The information remains in a file with the agency.

[*English*]

I'm turning to my colleague.

I believe it's seven years if we....

[*Translation*]

I can provide you with the details. The information is retained for a number of years.

When we check a device that shows no violations of the law, we do not store any data. We simply give the device back to the traveller.

Ms. Karine Trudel: In your speech, you said that, depending on the situation, you had to share information with other agencies, including the police. You mentioned Immigration, Refugees and Citizenship Canada.

Mr. Martin Bolduc: It's not necessarily the information collected from a cellphone. It is information that is collected routinely, basically the information on page 2 of your passport. It is routinely sent to our colleagues at Immigration, Refugees and Citizenship Canada. Some data are also shared with Statistics Canada for statistical purposes.

Your question was about the information that we retrieve from a cellular device. In the case of an active investigation, information may be forwarded to our colleagues at the RCMP and the Canadian Security Intelligence Service for further investigation.

Ms. Karine Trudel: I would like to know what data are being shared with Statistics Canada. Is it the number of passengers, for example?

Mr. Martin Bolduc: Yes, it may be the number of passengers or whether they are returning residents or visitors. I'm answering from memory, but let's say it's usually very general information.

Ms. Karine Trudel: Okay.

Mr. Martin Bolduc: That's what allows Statistics Canada to regularly publish the number of foreign visitors to Canada.

Ms. Karine Trudel: I'd like to go back to something else I read in your document. By the way, thank you very much for providing us with your written presentation. You say that, in the event of any questions or discrepancies, individuals can request that the CBSA amend the information.

In which cases can requests be made to amend information? Can someone do it because they felt wronged because you asked to check their cellphone?

Mr. Martin Bolduc: In my opening remarks, it is important to distinguish between cellphones, which are one segment of a multitude of activities, and our information sharing. Mr. Mundie can give you an example, but I think we have to distinguish between the two. Not everything is about cellphones.

[*English*]

Mr. Robert Mundie: Generally speaking, if you have a dispute from an experience you've had at the border, we have a recourse directorate within the corporate affairs branch that will receive a complaint or a compliment, and it will be appropriately handled through the organization and you'll get a response. You can also go through your member of Parliament or write the minister. There are other ways of bringing this to our attention.

[*Translation*]

Ms. Karine Trudel: Are those measures posted? If you want to know how to file a complaint, can you find the procedure on the Internet? Is it accessible to the public?

[*English*]

Mr. Robert Mundie: Yes, you can find it on our website. It gives the details. You can either mail in a complaint or you can submit it electronically.

● (1600)

[*Translation*]

Mr. Martin Bolduc: In the window, there is a place for complaints and another for compliments, which we also accept.

Ms. Karine Trudel: Of course, compliments are always welcome.

Thank you.

[*English*]

The Chair: Next is Mr. Erskine-Smith, for seven minutes.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): I take it, from a question put by my colleague Mr. Gourde, that you'll provide the committee with the number of searches of cellphones that the CBSA has conducted over the last number of years—say the last three years.

Mr. Martin Bolduc: No, right now we're not tracking separately how many cellphone searches we have done. I asked my team to start tracking those—

Mr. Nathaniel Erskine-Smith: —as of today?

Mr. Martin Bolduc: No, that request was made a few weeks ago.

Mr. Nathaniel Erskine-Smith: Okay.

Mr. Martin Bolduc: I want to make sure that we have the ability to track systematically and with rigour, so that whatever becomes public is solid.

What I committed to do was on the question, when did we start looking into cellphones, and I don't have that answer.

Mr. Nathaniel Erskine-Smith: Okay. So that I don't forget to ask six months from now, when we hit the six-month mark and you have the number of searches conducted over a six-month period, perhaps you could provide that number to the committee.

Mr. Martin Bolduc: Sure. It's quite easy to do so.

Mr. Nathaniel Erskine-Smith: Thanks very much.

It would also be interesting, as you track the number of searches you've done, to have you track how many searches turned into something substantive. It's interesting to note that Mr. Stroud said that we don't do this at the airports, that they don't feel it's necessary. It's curious that we would feel it's necessary to do it at the border. It would be good to know what percentage of cases leads into something.

Mr. Martin Bolduc: That's fair, recognizing that it may lead to something not immediately, but further down the road.

Mr. Nathaniel Erskine-Smith: It's interesting that you say that. I understand from the operational bulletin that you are searching for customs-related purposes principally, and not for any secondary purpose. How, then, would it lead to something down the road?

Mr. Martin Bolduc: I'm just using an example in a general sense. If we come across a traveller who has propaganda on his cellphone, that may lead to having reasonable grounds to believe that the person might be involved in other activities. When I referred to your colleague's question earlier about case-by-case sharing of our information with colleagues from the RCMP and CSIS....

Mr. Nathaniel Erskine-Smith: It's not, then, that you are searching for it in the first instance, but that if you find it in the course of an otherwise legitimate search, you might share it with other agencies.

That gets to my next question. What would prompt a search? I see language in the operational bulletin, "multiplicity of indicators". Maybe you could give us examples. What does a multiplicity of indicators mean? Give us a multiplicity of indicators.

Mr. Martin Bolduc: Without going into too many details, it could be your behaviour, the way you answer a question asked by the officer, the coding you have on your suitcase that doesn't match where you are coming from, or the fact that your ticket was purchased the day before. That's what we mean by a multiplicity of factors.

Mr. Nathaniel Erskine-Smith: It's interesting that you use those examples, because I take from the operational bulletin that searches are only to be conducted for customs-related purposes. How are those indicators relevant to customs-related purposes?

Mr. Martin Bolduc: Again, we have to dissociate the search of a cellphone from the secondary search we conduct. As I explained before, some people are referred for what we call a secondary examination. You go to a kiosk, or talk to the first officer and you are referred with your luggage to a secondary area. We will start going through your bags and asking you questions to see if there is any contravention of the act. If we find evidence that may cause the officer to believe there might be contravention, one of the things we can do is ask to look into your cellphone.

Mr. Nathaniel Erskine-Smith: The cellphone is typically near the end of an investigation, then.

Mr. Martin Bolduc: We carry out an examination. We are in a public forum, so I won't divulge all our techniques, but we make our examination in a progressive fashion. Unless you show up in the secondary area and you disclose to the officer that you have contraband with you—that will expedite the search—but usually, people don't come clean when they see the officer.

Mr. Nathaniel Erskine-Smith: CCLA was before us, and in answer to one of my questions, they delivered a factum arguing that the search under the Customs Act of an electronic device without a warrant is unconstitutional. Do you have a constitutional analysis of warrantless searches of electronic devices at the border? Has that been conducted by the CBSA?

● (1605)

Mr. Martin Bolduc: I am not aware of that.

Mr. Nathaniel Erskine-Smith: If there is such an analysis, could you provide it to the committee, or see if the committee can have access to that?

Mr. Martin Bolduc: Yes.

Mr. Nathaniel Erskine-Smith: Do your officers download and store any information from a cellphone?

Mr. Martin Bolduc: Not at ports of entry.

Mr. Nathaniel Erskine-Smith: The information is not retained whatsoever.

Mr. Martin Bolduc: No, not by our officers at the port of entry.

If we find an infraction and we start a seizure, yes, the personal device could be seized and could be sent to our criminal investigator, who will decide what to do with it. From the border services officer perspective, though, we don't store information from the cellphone at the counter.

Mr. Nathaniel Erskine-Smith: I don't know what familiarity you have in dealings with your American counterparts, but we've heard some testimony from the OPC and I have certainly read in the media that those who have acknowledged smoking cannabis, or those who have certain health concerns, have been turned away at the U.S. border. What information is being shared with American counterparts in this instance, and do you have concerns, as we legalize cannabis, that American border officials will be turning Canadians away?

Mr. Martin Bolduc: Today, it's not part of our regular questionnaire. Depending on the outcome of the cannabis legislation.... Right now, the way that it's drafted, cannabis import or export remains prohibited in Canada.

Mr. Nathaniel Erskine-Smith: Certainly, if I have used cannabis, I ought not to be turned away at the American border, one would think, especially if it's legalized. That is a concern to me and to my constituents. What can we do to prevent that from happening?

Mr. Martin Bolduc: Without knowing all the ins and outs of how our U.S. colleagues at the border operate, they do their inspection in a very similar fashion to how we do ours, in a progressive fashion. My advice to anybody who crosses an international border is to be truthful. If you are asked, you should tell the truth. But again—

Mr. Nathaniel Erskine-Smith: I appreciate that, but truthfulness in this case may mean I don't get into the U.S.

Thank you very much. I'm out of time.

The Chair: Mr. Blaney, for five minutes.

[*Translation*]

Hon. Steven Blaney (Bellechasse—Les Etchemins—Lévis, CPC): Mr. Chair, thank you for welcoming me to the committee.

My thanks to the witnesses for being here today.

Essentially, my questions will deal with the changes that are likely to come after Bill C-21 receives royal assent. I would like to know what will change in the entry/exit initiative, compared to your current activities.

My question goes to Mr. Bolduc.

You mentioned that, when people who appear at the border have a visa, you begin to collect information. Is that the case?

Mr. Martin Bolduc: With certain visas issued by our colleagues at Immigration, Refugees and Citizenship Canada, the foreign visa officer takes a biometric measurement, which is to say fingerprints, so that it is possible to confirm that a person arriving at a Canadian point of entry is really the person to whom the visa has been issued. We then confirm the authenticity of the fingerprints. There is a validation system to make sure that it really is the right person.

Hon. Steven Blaney: So, when foreigners want to come to Canada and apply for visas, they provide their passports and their fingerprints. When they arrive at the border, you check those two items of information, the passport and the fingerprints. Is that what you are saying?

Mr. Martin Bolduc: Exactly. That is the case for people from a certain number of countries. I do not remember all the countries on the list.

Hon. Steven Blaney: Okay.

I missed your presentation and I apologize for that, but can you tell me whether, as far as the Canadian Air Transport Security Authority is concerned, there is any difference in the baggage handling in cases where there are visas? Does the fact that a person has a visa have any effect on the treatment they receive at the airport?

[*English*]

Mr. John Stroud: I don't believe so.

Our mandate is pretty straightforward. There's a list of prohibited items prepared by Transport Canada, and we screen everybody to the same standard. We apply the rules uniformly.

● (1610)

[*Translation*]

Hon. Steven Blaney: Great, thank you.

Now, if we assume that the entry/exit initiative is passed, can you explain to us how things will be different? As it will affect Canadian citizens, can you tell us what differences will be involved?

Afterwards, I will perhaps deal with the privacy issues.

Mr. Martin Bolduc: At the moment, we exchange information with our American colleagues on foreign nationals, permanent residents and American citizens. When a permanent resident of Canada enters the United States, it means that they are leaving Canada. When that person comes back to the land border, coming back into Canada means leaving the United States. That information is exchanged digitally, almost immediately, in less than about 15 minutes. Essentially, the information exchanged is the information on page 2 of the passport: name, citizenship and date of birth. Then the date on which the person entered or left is added, plus the place where that occurred.

The difference the bill will make is that it gives us the legal authority to gather information on Canadian citizens and, in the case of the land border, to exchange that information with the United States. We will also be able to gather information on all travellers leaving Canada by air. At the moment, the agency does not gather that information. That will not be exchanged with the Americans. It will be useful only to the Government of Canada.

Hon. Steven Blaney: Do you not already gather that information for some types of citizens or travellers?

Mr. Martin Bolduc: Not if they are travelling by air, no.

Hon. Steven Blaney: If they are travelling by land?

Mr. Martin Bolduc: At the land border, yes, we gather that information for the three groups.

However, on entry, we gather information on everyone arriving in Canada, whatever their nationality. What the bill will make it possible for us to do is to gather information on Canadians at all land borders, and on all travellers when they leave by air. As I said, the information obtained at the land border will be exchanged with the Americans, but not information when travel is by air.

Hon. Steven Blaney: Okay. Are you going to—

[*English*]

The Chair: Mr. Blaney, that's time.

[*Translation*]

Hon. Steven Blaney: Okay.

Thank you.

[*English*]

The Chair: Next is MP Dubourg, for five minutes.

[*Translation*]

Mr. Emmanuel Dubourg (Bourassa, Lib.): Thank you, Mr. Chair.

Now it is my turn to welcome you this afternoon and to thank you for coming to our committee.

My first question goes to John Stroud.

We understand the role of customs, of course, but could you tell us about the mandate of the Canadian Air Transport Security Authority, and about how you become involved? Travellers go through customs, but you talked about the things people have in their luggage. Could you please clarify your mandate for us, as it relates to customs, and to travellers?

[*English*]

Mr. John Stroud: In terms of customs, CATSA doesn't have a role. CATSA is responsible for passengers who are departing. Our role is very prescribed. Transport Canada is our regulator, and we're responsible for aviation security.

Essentially, Transport prepares a list of prohibited items that are not permitted on the plane. Our job is to detect them. We do that by screening passengers and their baggage, whether it's carry-on or checked luggage.

We also have a screening program for airport workers. The people who work at the airport who go from the public side to the secure side have to go through certain checkpoints, and we screen them as well. If we find a prohibited item, then we intercept it. That is essentially our mandate.

● (1615)

[*Translation*]

Mr. Emmanuel Dubourg: Okay. Thank you.

Does that mean that, while your officers are doing that checking, if they find electronic devices, such as iPads or cellphones, that are not prohibited, not unadvisable to have, on board, they do not touch them? Do they leave those devices to the people from customs?

[*English*]

Mr. John Stroud: We have to inspect the devices. We ask that the device be able to be powered on. That's what we want to verify, and that's a check to make sure that it's.... If it's a phone, and you can turn it on, you verify that it's a phone.

Our concern is not whether there is data on it. Our concern is whether there is a threat item hidden in the phone. We're looking for, say, explosives.

[*Translation*]

Mr. Emmanuel Dubourg: In the cases when, as you say, you find a threat in one of those electronic devices, what do you do right away, compared to the customs officers, who are also at the airport at the same time as you? What contact do you have with the Canada Border Services Agency?

[*English*]

Mr. John Stroud: We don't have contact with CBSA. We're worried about outgoing passengers. CBSA is responsible for incoming passengers.

If we find a phone with a threat item, then we intercept it to make sure that it doesn't get on the plane. That's our responsibility.

[*Translation*]

Mr. Emmanuel Dubourg: Thank you.

I would like to ask Mr. Bolduc a very quick question, given that his office is in the province of Quebec, I believe.

You say that you are going to look for information in people's passports. This summer, we saw a massive influx of migrants arriving at the border and I assume that some of those people had no passport. How did you go about ensuring the safety of Canadians and of those people arriving in the country?

Mr. Martin Bolduc: Thank you for the question.

Although I do not have the statistics with me, I can tell you that the great majority of those who arrived—and are still arriving, unfortunately—had a piece of identification or a document. When people cross between two points of entry, as we have been able to see on many occasions in the news, they are intercepted by the RCMP. They do a preliminary background check to make sure that the people do not pose a threat. They are then taken to our point of entry, where we can continue the checking, which of course includes taking fingerprints, so that we can determine whether there is anything else in their background.

I should tell you that the checking has multiple stages. Canadians can be assured that, once we release people, they do not pose a threat. If we consider that there is a threat to security, if we are not able to identify the people in front of us, or if we believe that, for whatever reason, those people will not show up for further procedures, we always have the option of detaining them.

Basically, those are the steps we follow.

[*English*]

The Chair: Thank you MP Dubourg.

We are returning to MP Blaney, for another five minutes.

Hon. Steven Blaney: My first question would be for Mr. Mundie.

With the implementation of the entry/exit initiative, is there any change in your operation? Will it have any impact?

Mr. John Stroud: I'm sorry, was the question for me?

Hon. Steven Blaney: Sorry, I called you Mr. Mundie. You're Mr. Stroud. I'm sorry. I should wear glasses now.

● (1620)

Mr. John Stroud: I'm sorry, could you repeat the question?

Hon. Steven Blaney: My question is on the entry/exit initiative. It has zero impact on you.

Mr. John Stroud: That's correct.

[*Translation*]

Hon. Steven Blaney: Let me go back to the officials from the Canada Border Services Agency.

Basically, you already have that information. However, when the entry/exit initiative comes into effect, will it change the protocols that already exist with various countries?

Mr. Martin Bolduc: In terms of the information sharing protocol with the Americans, the update is necessary in order to include Canadians, if the bill gets royal assent. Canadians are not included in the protocol at the moment.

That will change what we do. Currently, the agency does not gather information on exits from Canada. Once the bill has received royal assent, the agency will have the authority to gather information on people leaving Canada.

Hon. Steven Blaney: Do you not already do that for some categories of people leaving Canada?

Mr. Martin Bolduc: We do at the land borders, but not at airports.

Hon. Steven Blaney: Okay.

At the moment, what kinds of people do you collect information on when they leave at a land border?

Mr. Martin Bolduc: Permanent residents and foreign nationals.

Hon. Steven Blaney: Right. That's what you told me.

So you are going to expand your pool, but the memoranda will be of the same type that you already have in terms of transferring information between governments in Canada or with foreign agencies, if I may use the term.

Mr. Martin Bolduc: We are going to broaden the base at land borders in terms of the exchange with the Americans. In addition, there will be a new way of collecting information on air travel, strictly for the Government of Canada.

Hon. Steven Blaney: Okay. Even that will be done with the same memoranda, to an extent.

Mr. Dubourg brought up the events that happened on the border this summer. I would like to go into that more deeply.

Do you have recent figures for us today about the number of illegal migrants that we have received on the border to this point?

Mr. Martin Bolduc: I do not have those figures with me, but I will be happy to provide them to you as soon as I get back to my office.

Hon. Steven Blaney: Okay.

Do you feel that you have enough human resources to deal with this influx?

Mr. Martin Bolduc: The agency has used the resources it has. We have deployed resources from other regions. They have come to help mostly at our crossing at Saint-Bernard-de-Lacolle, where we receive most of the people. People from other regions are providing us with assistance even today.

Of course, we re-evaluate our needs on a daily basis. As you know, the number of people crossing between points of entries fluctuates each day. We make sure that we have enough resources to deal with the influx.

Hon. Steven Blaney: Okay, thank you.

[*English*]

The Chair: Thank you.

Next, for five minutes, is MP Long.

Mr. Wayne Long (Saint John—Rothesay, Lib.): Thank you to our guests this afternoon.

I want to circle back on one thing with respect to the number of phones being searched. I read somewhere—and I do apologize; I don't have it in front of me—that the number of phones being searched is growing exponentially. It went from 5,000 to 50,000 to so many thousands per month.

Do you have any information on the growth of searches that you're doing?

Mr. Martin Bolduc: I think the number you may be referring to —because I saw the same thing in the media—is information coming from the United States.

Unfortunately, in Canada, the CBSA doesn't make any distinctions between a secondary examination that is limited to questions to a traveller, to luggage searches, to other searches. As I said earlier, because of the interest in this question, I've asked my team to come up with a procedure so we can track systematically and with rigour those specific examinations.

Mr. Wayne Long: Thank you.

I had an experience recently crossing the American border when we were asked to leave our phones in our vehicle. They were obviously searched because we had to open them. Are you obligated to tell people that you went through their phones? In other words, if a phone was left in the car and you took the phone, are you obligated to tell those people that you searched their cellphone?

● (1625)

Mr. Martin Bolduc: I can't speak to U.S. policies. I can tell you that the CBSA policy is that officers are instructed as to what they can do and how they can do it. The fact that we need to ask the traveller for the password and have the ability to unlock the phone ourselves wouldn't be done without your knowledge that we're going through your cellphone.

Mr. Wayne Long: Is it just a physical manual search of the phone? Is the phone hooked up to devices? How do you search a phone?

Mr. Martin Bolduc: I think it's really important that it's made very clear what we do. Essentially, we take the phone, have the passenger provide us with the password to unlock it, and the first thing we do is put it in airplane mode.

Mr. Wayne Long: You do?

Mr. Martin Bolduc: Yes.

Mr. Wayne Long: You don't ask the person to put it in?

Mr. Martin Bolduc: No.

Mr. Wayne Long: You do it. Okay.

Mr. Martin Bolduc: Because if there is evidence on the phone and I turn it back to the traveller, there's a possibility that the evidence will disappear. Our officers will deactivate the Wi-Fi, any network connection. When it's on airplane mode—you've travelled —there is no cellphone provider, no Wi-Fi, there's nothing. It's only what's on the phone. Then the officer will go through the phone, depending on what he's looking for, based on what he was able to gather during the interview with the traveller.

Mr. Wayne Long: Sure. I don't think it's any secret to anybody here that our lives are on our phones now. It's more than just texts. It's our banking information, our insurance information, what have you.

I read an article recently and the headline was that the U.S. Department of Homeland Security will start collecting social and search data on every immigrant's phone coming into the U.S., and that includes naturalized citizens, those with a green card, etc. What are your thoughts? Do you think that's overkill? Obviously we're in a climate where the borders are certainly being tightened up with our friends to the south. Do you think that's too much? What are your plans for immigrants coming into Canada?

Mr. Martin Bolduc: This is not the CBSA's policy. We're not contemplating something similar to what you describe is occurring in the U.S.

It would be inappropriate for me to comment on U.S. legislation, laws, and policies. They are a sovereign country. They can legislate the way they want.

Mr. Wayne Long: Sure.

Mr. Martin Bolduc: It's for our front line. We have 5,800 border services officers who protect the border every day. Striking the right balance between facilitation and security in the threat environment in which we operate, and it's no different for the screening officer for CATSA, is a daily challenge. It's not an easy job today, because if you miss one, you're doomed.

It's striking the right balance, but I can tell you that we're very clear and our officers understand that. Everything we do, we do through a privacy lens. We're very mindful of that.

Mr. Wayne Long: Thank you very much.

The Chair: Thank you to the witnesses.

From a person who travels a lot, we appreciate what you do in keeping us safe. It's always a balance between getting too much information and not enough. We appreciate your service and your members' service to us as members of Parliament and travellers.

Thank you for coming today.

I'll suspend for five minutes until we have our next witnesses come in.

● (1625)

(Pause)

● (1630)

The Chair: We'll bring the meeting back to order.

Before I introduce everybody, the Canadian Bar Association has submitted a full brief in English and the executive summary in French, so I need to ask for unanimous consent to allow those documents to be circulated to our committee.

Do I have unanimous consent?

Some hon. members: Agreed.

The Chair: Thank you, everyone. We'll have those documents circulated. I'll introduce our guests while I wait for that to happen.

Welcome again to the Standing Committee on Access to Information, Privacy and Ethics, meeting number 69. Pursuant to Standing Order 108(3)(h)(vii), this is a study of the privacy of Canadians at airports, borders, and travelling in the United States.

From the Canadian Bar Association we have Cyndee Todgham Cherniak, member-at-large for commodity tax, customs and trade; and David Fraser, executive member, privacy and access law section.

As individuals we have Michael Geist, Canada research chair in Internet and e-commerce law in the faculty of law at the University of Ottawa; and Kris Klein, partner, nNovation LLP.

We'll start off with the Canadian Bar Association, for 10 minutes.

● (1635)

Mr. David Fraser (Executive Member, Privacy and Access Law Section, Canadian Bar Association): Mr. Chair and honourable members, we appreciate your invitation and are very pleased to be here today on behalf of the privacy and access law section, immigration law section, and commodity tax, customs, and trade sections of the Canadian Bar Association, as well as the Canadian Corporate Counsel Association and the ethics subcommittee of the policy committee of the CBA board, to present views on the privacy of Canadians at airports, borders, and travelling in the United States.

The CBA is a national association of 36,000 lawyers, law students, notaries, and academics. An important aspect of the CBA's mandate is seeking improvements in the law and the administration of justice. This is what brings us before you today.

My name is David Fraser. I'm an executive member of the privacy and access law section. I'll be representing the CBA sections that prepared our submissions to the committee on this issue, along with Cyndee Todgham Cherniak, who is here with me today. Cyndee is an executive member of the commodity tax, customs, and trade section.

Some information collection is necessary, and certainly expected, at the border; there is really no doubt about that. Our principal concern and the concern of the Canadian Bar Association is mainly about where the line is drawn and where the line is moving and how the fundamental principles in our charter may be left behind as this line is moved. We have commented in our document on both Bill C-21, related to Customs Act amendments, and Bill C-23, related to pre-clearance.

In Bill C-21, we're very concerned about open-ended discretion being given to the CBSA to examine people leaving Canada.

In Bill C-23, we're very concerned about what may be a general disregard of the charter and Canadian norms, when non-Canadian law enforcement officers are empowered to conduct invasive examinations in Canada. We're concerned about broad powers to interrogate those who choose to withdraw from entering the United States. We're concerned that U.S. officers can, for example, perform a strip search in Canada over the objection of a CBSA officer. We're concerned generally about a lack of accountability.

Obviously, electronic devices and the privacy of the contents are of great concern. As lawyers, we're seeing and hearing about searches of digital devices becoming much more commonplace. The CBSA is essentially using suitcase law, developed before the 1980s, to justify a massive intrusion into digital information.

The Customs Act provisions that are at issue were drafted before the 1980s, before laptops, before smart phones, and before thumb drives. In the meantime, the Supreme Court of Canada has said very strongly that all Canadians have an extremely acute privacy interest in the contents of computers, laptops, and smart phones. This has apparently fallen on deaf ears within the CBSA. People travel with a huge quantity of personal information, and the CBSA say that they can go through it legally on a whim. They say they don't, but the law, if applied as they say it is, would allow them to do it on a whim. We say this is likely unconstitutional and needs to be very closely examined by Parliament.

We also have concerns about information sharing, in that the devil is in the details: questions about information sharing between administrative agencies and law enforcement, between one law enforcement agency and another, between federal and provincial agencies, between private companies and governments, and vice versa. We think this needs to be scrutinized very closely, particularly as this information is moving around at a rapid pace. Then you overlay on top of this information sharing between governments, which of course is becoming even more common and something we need to be very concerned about.

My colleague Cyndee will introduce the balance of the issues that we've addressed.

● (1640)

Ms. Cyndee Todgham Cherniak (Member-at-Large, Commodity Tax, Customs and Trade, Canadian Bar Association): An issue of great importance to the Canadian Bar Association is solicitor-client privilege. Solicitor-client privilege is fundamental to the proper functioning of the Canadian legal system. As a result, steps must be taken to ensure that solicitor-client privilege is protected at Canadian airports, Canadian ports of entry, and U.S. pre-clearance areas on Canadian soil.

The Supreme Court of Canada has repeatedly emphasized that solicitor-client privilege must remain as close to absolute as possible and should not be interfered with unless absolutely necessary. In the rare case of necessity, there must be explicit statutory language stating that privilege can be interfered with, which must be accompanied by legislative safeguards. Most people, including lawyers and clients, travel with solicitor-client privileged documents on their laptops, on their smart phones, on USB keys, and so on.

It is essential that the CBSA and U.S. customs, when operating in Canada, maintain a transparent policy and process to address solicitor-client privilege. When solicitor-client privilege is claimed, Canadian courts, not the CBSA or U.S. custom officers, should make the determination of the validity of such claims.

The Canadian Bar Association has made a number of recommendations in the submissions they have provided to the committee.

One, the CBA recommends the creation of a working group with representatives from the Canadian Bar Association, Justice Canada, and the CBSA to collaborate in the development of a defined policy for examination at the Canadian border where solicitor-client protected information is involved.

Two, the CBA recommends that the CBSA's policy on solicitor-client privilege be made publicly available on the CBSA website. Remarkably, it is not available at the current time for all to see and to hold the CBSA accountable. The CBA has made a number of recommendations in the submissions concerning the content of the current operational bulletin on solicitor-client privilege. Please review those submissions and our recommendations.

This committee should strongly recommend that the Canadian Ggvernment require U.S. customs to have a transparent and available written policy on solicitor-client privilege that is applicable to all pre-clearance examinations on Canadian soil. The CBA submissions also address oversight of the CBSA in areas such as information sharing by the CBSA with other government departments and other countries. Robust accountability mechanisms are crucial to the legitimacy and efficacy of our national security agencies as well as to public confidence in them.

This committee should recommend that the Government of Canada put effective CBSA oversight and complaints mechanisms in place, and that a transparent mechanism and process for Canadians and Canadian residents be put in place to challenge information collected about them at airports and the border. Any oversight model must incorporate a robust review mechanism. There should be verifiable procedures to ensure that any improperly obtained information is expunged from the CBSA and U.S. customs databases.

I would more than welcome any of your questions.

The Chair: Thank you.

We'll move to Mr. Geist, as an individual.

Dr. Michael Geist (Canada Research Chair in Internet and E-commerce Law, Faculty of Law, University of Ottawa, As an Individual): Thanks very much. Good afternoon.

My name is Michael Geist. I am a law professor at the University of Ottawa, where I hold the Canada research chair in Internet and e-commerce law. I have appeared many times before this committee on privacy issues, although not always in such a nice room. As always, I appear in a personal capacity representing only my own views.

I'm grateful to the committee for its commitment to privacy and its efforts to highlight the privacy issues associated with our airports and border crossings. The media has regularly covered these issues, as you know. There are fears of device searches at borders, stories of information sharing that goes beyond most reasonable expectations, and mounting concerns about the approach of U.S. law and border officials with respect to the privacy rights of non-citizens and non-permanent residents.

These stories hit home, as we saw just a few minutes ago with Mr. Long in the last panel. Everyone seems to have their own story. Recent incidents include one involving a Quebec resident who didn't want to provide his cellphone password. It was searched at the Canadian border in Halifax. He was ultimately arrested for not giving a passcode when asked. The argument was that he was hindering an investigation. In another incident, a Canadian man was denied entry into the U.S. after customs and border patrol officers demanded that he open his phone and provide access to his apps. There was yet another incident involving a Canadian photojournalist who was inspected on his way to Standing Rock. Officials photocopied pages of his personal journal and asked for three mobile phone passwords, which he said he could not disclose because of his ethical obligation to protect his sources. The phones were taken and returned hours later with tamper tape covering the SIM cards, suggesting the cards had been removed and copied.

The privacy associated with border crossings now seemingly captures everyone's attention. I think it's worth asking why. I think there are at least three sources of concern that help point to potential policy solutions.

First, there is the feeling amongst many that border crossings represent no-privacy zones in which it feels as if officials are entitled to demand whatever information they wish and can use whatever means to acquire it. I know of technical experts who regularly wipe their phones or establish border crossing social media accounts in order to counter fears of invasive searches, both physical and digital, when crossing the border.

Second, as these stories suggest, the search itself—and we've heard about this now from a number of people—has changed dramatically in recent years with the legal safeguards failing to keep pace. It's one thing to know that your belongings may be searched. Yet today, we all know that our devices and the information on them can tell a far more personal story, our social graph, our location history, our reading habits, our contacts, and our purchasing history. In searching this information, officials may literally be accessing just about everything about us. Doing so, potentially without appropriate safeguards, understandably leaves many feeling vulnerable. The data indicates, as we heard on the last panel, that at least in the United States, these forms of searches are increasing rapidly. In fact, in the United States, there have been some policies that have posited that such searches can occur with or without reasonable suspicion.

Third, it may not be comfortable to say, but part of the concern stems from the fact that the U.S. border is by order of magnitude the most significant one for Canadians. This is not solely a comment about the current U.S. administration. Rather, it reflects long-standing concerns about the U.S. approach to privacy and fears that U.S. privacy protections may be weaker than those found in Canada. For example, the enactment of the USA Patriot Act after 9/11 opened the door to extensive access to personal information without traditional safeguards. Over 10 years later, the Snowden revelations reinforced the massive data gathering efforts of signals intelligence and law enforcement agencies. Most recently, the Trump administration's executive order aimed at reversing efforts to establish privacy protections for non-U.S. citizens and residents again placed the issue in the spotlight.

What is there to do about it? I thought the Privacy Commissioner of Canada, who raised issues such as information sharing across borders, the U.S. executive order, and CBSA searches provided excellent context and advice.

I'd like to briefly provide additional comments on four issues.

First, I think this committee and several of these committees have done excellent work on Privacy Act reform. As you know, it has been an issue that has regularly come up before this committee. There are few areas within Canadian privacy that are more overdue for updating. Indeed, there have been consistent and persistent calls for reforms for decades.

● (1645)

One of the methods of addressing some of the airport privacy concerns in Canada may be through the Privacy Act. Your proposed reforms to provide the Office of the Privacy Commissioner of Canada with greater powers would empower that office to examine border issues in a more comprehensive manner and open the door to more careful reviews of cross-border sharing arrangements. You recommended the reforms; now we need action.

Second, information sharing within government—we just heard about it from Mr. Fraser—remains a source of concern. Indeed, some of the most notable anecdotal stories involving abuses or questionable conduct at the border arise due to information sharing between governments or government departments. The Privacy Act and the OPC are supposed to create safeguards against misuse of personal information, or the use of information for purposes for which it was not collected. However, we have witnessed mounting pressure in recent years for more information sharing between governments and government departments.

Bill C-51, which we all know garnered widespread criticism, featured a significant expansion of government sharing of information, undermining, I would argue, the effectiveness of the Privacy Act. Unfortunately, the information-sharing provisions as they were amended in that bill were only modestly changed. Information sharing was considered a feature, not a bug, and I should note that included the Liberal Party when it was in opposition.

Bill C-59, which seeks to amend Bill C-51, leaves many of the information-sharing provisions intact. There are two needs here that must be reconciled. One, I think we all recognize that government needs to be able to use the information it collects in a reasonable and efficient manner. Two, the public needs confidence that its information will not be misused. That confidence comes from legislative safeguards and effective oversight. There is reason to believe we do not yet have the right balance.

Third, as the Privacy Commissioner of Canada has discussed, Canadian law must apply on Canadian soil when it comes to these issues, particularly the charter. Reducing so-called friction at the border is a laudable goal. No traveller wants long lines or lengthy delays, and that of course applies in a commercial context as well. However, expediency has a price, and sacrificing the Canadian Charter of Rights on Canadian soil is, in my view, a bad bargain. The Supreme Court of Canada has upheld unauthorized searches of devices, and those principles should apply on Canadian soil in a like manner at the border.

Fourth, with the NAFTA negotiations ongoing this week in Ottawa, I think it is important to link those trade talks with this issue. While there is no airport privacy chapter in the agreement, at least that I'm aware of, NAFTA touches on many of these related issues. There will be pressure—we know there is pressure—to speed up border crossings in the name of increased trade. Further, the digital trade chapter, formerly the e-commerce chapter, is likely to include provisions on data localization, prohibiting some of the data localization, and restrictions on data transfers. NAFTA, of course, is not a privacy deal, but the reverberations from the agreement will be felt in the privacy world.

The European Union has regularly linked privacy and data protection with trade. We ought to do the same, recognizing that these issues are linked and that the policy recommendations that come out of this committee on this issue need to make their way into the negotiations. In fact, I'd go even further by noting that the U.S. now seeks to accord the Europeans with privacy protections under the privacy shield. Other countries, such as Australia during the TPP negotiations, sought to ensure that Australians enjoyed the same level of protection. Surely, Canada can use the NAFTA discussions to ensure that the same kind of protection afforded to citizens of other countries outside the United States is afforded, as well, to Canadians.

I look forward to your questions.

● (1650)

The Chair: Thank you, Mr. Geist.

Now we'll go to Mr. Klein, for 10 minutes.

Mr. Kris Klein (Partner, nNovation LLP, As an Individual): Thank you for having me.

When I teach privacy law, one of the first things we do at the beginning of the term is have a discussion about reasonable expectation of privacy and what it is. It's always a great conversation, especially amongst the budding young law students, who are keen to say you have a reasonable expectation of privacy in everything. They want to say it's everywhere, but it isn't.

That is why you are having this discussion today. On the one hand we have our cellphones, and we've heard testimony already saying that obviously we have a great expectation of privacy in our cellphone. We've even had the Supreme Court say the same thing, that on our devices we have a greater expectation of privacy.

On the other hand we have the borders, and—no joke—the courts in Canada have been strong in their position that we have zero expectation of privacy at the border. That's something the courts have said. Here are a couple of quotes from an Ontario Court of Appeal case from 2006:

> No one entering Canada reasonably expects to be left alone by the state, or to have the right to choose whether to answer questions routinely asked of persons seeking entry to Canada. ...The state is expected and required to interfere with the personal autonomy and privacy of persons seeking entry into Canada. Persons seeking entry are expected to submit to and co-operate with that state intrusion in exchange for entry into Canada.

We have these two competing forces, and I applaud the committee for trying to come to terms with it and come up with some meaningful recommendations. We're better off focusing on what we are doing here and some real solutions that we can impose here in Canada, as opposed to trying to figure out what to do to fix Canadian privacy rights in the United States, which is a pretty hard task to do from here.

Now the Privacy Commissioner has made a couple of recommendations in this respect, and I applaud them. For example, and Mr. Geist alluded to this, if Europeans have the privacy shield protecting them, why doesn't Canada have something similar? The starting point is the Judicial Redress Act in the United States, and the Privacy Commissioner has made a comment about this: it would be a simple fix just to list Canada as one of the countries that is afforded protection under this act in the United States. So it's not to say there is nothing that can be done to help Canadians while they are abroad; it's just that we have to recognize that if you are abroad, your privacy rights are not going to be the same as when you are at home.

The last point is let's concentrate on what we can do at home, and I won't reiterate it because I thought Mr. Geist said it really well: Privacy Act reform. Let's get our own house in order. This act is old, and it is in dire need of modernization. I'll end it there.

● (1655)

The Chair: Thank you.

We'll go to questions, starting with MP Erskine-Smith for seven minutes.

Mr. Nathaniel Erskine-Smith: We just had the CBSA here, and it was interesting to hear that the CBSA engages in cellphone searches at the border but not at airports. It strikes me as very odd that we need to search cellphones pursuant to the Customs Act, but not for other reasons due to border security. I just wonder if you find that odd as well.

Mr. David Fraser: I'm happy to comment on it, but not wearing my CBA hat. CBSA are the people who control the borders and who and what comes in, and CATSA are the people who scan people who get on planes to make sure they don't have bombs, knives, guns, and things like that. They don't really care what's on your phone, because that's not going to blow up and harm an aircraft. So they have some very significantly different roles. They all are involved in security along the continuum, but they have very different jobs. That might not have been sufficiently clear from their comments.

Mr. Nathaniel Erskine-Smith: Well, it wasn't sufficiently clear because when CBSA was asked for examples of what might be found on cellphones, they used examples like propaganda, which strikes me as actually very important for border security officials at airports. So it's still not clear to me for that reason.

Another example they used was in relation to child pornography, which should be of concern to all Canadians whether someone is crossing at the border or at an airport. They didn't actually give great indications of what they might find on a cellphone, other than a receipt perhaps. It's curious to me that searching cellphones for a receipt seems like a very unimportant thing when privacy in a cellphone is so very important.

Ms. Cyndee Todgham Cherniak: Again, I don't have my CBA hat on in answering your question; I have an individual hat on. I am a customs lawyer. I deal with people who get their NEXUS passes taken away on a regular basis, and I can tell you that the CBSA does look at cellphones and laptops at airports in addition to border crossings. There may have been a misunderstanding—

Mr. Nathaniel Erskine-Smith: I see, okay. I understand.

Ms. Cyndee Todgham Cherniak: —because you had CATSA and the CBSA at the same time, but I can assure you, that if you look at narrative reports by the CBSA, you will find many incidents of review of cellphones at airports.

Mr. Nathaniel Erskine-Smith: Maybe I'm phrasing the question incorrectly. Given the privacy implications of searching one's cellphone, it's odd to me that we're not searching it for important purposes, criminal law matters, actual security matters, but we're searching it for customs matters only, and that's what we're focused on. It seems very odd to me.

When it comes to the CBSA policy, are you familiar with the operational bulletin? Okay. When they were here before us, they said they don't retain the information, that they keep it on airplane mode. What in addition should they be doing? It strikes me that those are important steps that they are taking. What else should they be doing?

Mr. David Fraser: Overall in my experience, they're not consistent in applying the policy that they even have, and I've heard testimony of a CBSA officer who called it guidelines after justifying a search of a cellphone that was not placed into airplane mode.

So we have a law, the Customs Act, the provisions of which were drafted before the 1980s when none of this was contemplated, and the definition of a good includes a document, when at the time, generally, a document was referring to a bill of lading, so the document of title related to the widget, the box of whatever it is that you're bringing in. So according to their reading of the law, they can look through a cellphone; they can observe any document, and they can do whatever they want with it without any even suspicion, without any reasonable basis, and it's just part of the continuum of their secondary screening.

And they have a policy that says they only do it as part of an escalation, and they only do it if they have reasonable grounds to suspect or reasonable grounds to whatever, but the law that they're operating in doesn't do that.

● (1700)

Mr. Nathaniel Erskine-Smith: The operational bulletin uses language that I hadn't come across particularly as a lawyer, "multiplicity of indicators". There's an explanation we had from Mr. Bolduc, but it wasn't exactly clear to me what a multiplicity of indicators would be in relation to a contravention of the Customs Act, and there always has to be that relevance to contraventions of the Customs Act. In your view, what does multiplicity of indicators mean?

Mr. David Fraser: I can only refer back to what he said, which would be a number of things that would lead them to suspect more, so something such as you're nervous, you seem evasive, those sorts of things.

I think the connection of the Customs Act is if you bring something into Canada that is illegal in Canada under the Criminal Code, that's a violation of the Customs Act.

Mr. Nathaniel Erskine-Smith: On the solicitor-client privilege briefcase law, you say we have briefcase law and it's analog law and we need to move to digital law. If I'm a lawyer and I'm crossing the border with privileged documents in my briefcase, the CBSA can still search my briefcase, no?

Ms. Cyndee Todgham Cherniak: At the present time, the CBSA can search your briefcase. As a traveller, they can search your briefcase. As a lawyer, they can search your briefcase. According to the policy, if they come across documents marked "solicitor-client privilege", then they might stop the search. But how many of you the last time you wrote to your lawyer in an email had solicitor-client privilege in the subject line or in the document? Very few documents that lawyers receive have the words "solicitor-client privilege" on them.

Mr. Nathaniel Erskine-Smith: I would think very few lawyers are using an email that doesn't require an additional authorization that CBSA would not be asking for. Your recommendation that cellphones should not be treated as a good and should require a warrant to search, how would that work in practice? I'm crossing the border with my cellphone and they want to search my cellphone and now they require a warrant, but I need to cross that border.

Mr. David Fraser: Certainly what it would take is that they would have to develop more than the multiplicities of indicators. They would have to have reasonable grounds to suspect that a crime —or it could be also a violation of the Customs Act—has been, is being, or is about to be committed, and that searching the device would provide evidence of that, otherwise reasonable sort of criteria that are used in other circumstances.

It may well be that the reality is that people when asked will simply hand it over in order to get out of there. The simple reality is that at the borders when you're standing in line, you've gotten off a red-eye flight and you're exhausted and want to get through. But in terms—

Mr. Nathaniel Erskine-Smith: Just so I'm clear, what you have explained there suggests that rather than a multiplicity of indicators, it should be reasonable grounds.

Mr. David Fraser: Yes.

Mr. Nathaniel Erskine-Smith: Well, with respect to obtaining a warrant in real time when I want to cross the border, I'm trying to imagine that functioning in practice.

Mr. David Fraser: There is no doubt that there would be a delay —there is no doubt about that—although judges are standing by 24–7 to do telewarrants across Canada.

Mr. Nathaniel Erskine-Smith: Perhaps not for violations of the Customs Act, though.

Mr. David Fraser: Perhaps not.

Mr. Nathaniel Erskine-Smith: I think I'm out of time.

The Chair: Yes, you are.

Now we'll go to MP Blaney for seven minutes.

Hon. Steven Blaney: Thank you, Mr. Chair.

[*Translation*]

Welcome, everyone.

[*English*]

For the record, I'd like to say that I'm very proud to have introduced Bill C-51, the anti-terrorism act, and I sure sleep better at night. This being said, I also want to acknowledge that the Liberals tabled Bill C-21, the entry/exit initiative, and I'm glad to see the Canadian Bar Association is recommending that the government implement it. We agree on that.

In light of my former capacity, one thing I'd really like to hear you make recommendations on to this committee—and I will begin with you, Madam Cherniak—is the oversight of CBSA. It is my understanding that currently there is a recourse within CBSA. I'd like to hear more on that. You seem to have some ideas on the oversight of CBSA, and also on the review mechanism and the way people who feel they have not been dealt with properly could exert their rights.

Ms. Cyndee Todgham Cherniak: Based on my experience as a lawyer, there are a number of mechanisms already. There is a complaints process, but there is not a lot of back and forth with the complainer in that process. Also, it's going to the CBSA; it's not going to someone else looking at the actions of the CBSA.

The second mechanism is the recourse directorate. When a contravention has occurred, the recourse directorate is looking for a decision of the minister to overturn that contravention, or if a NEXUS pass has been taken away, confiscated and cancelled, a review of that process.

If you haven't had a contravention, though, you can't complain about the CBSA looking at your cellphone or your laptop. If someone who has had his or her cellphone reviewed without it leading to anything and then writes a complaint to the recourse directorate, the recourse directorate would say they have no jurisdiction to look at this because there is nothing for them to review. There is no provision of the Customs Act that authorizes them to do this.

There needs to be some mechanism in place to review the narrative reports of the officers, and the complaints. You have access to the complaint process, to the CBSA, not the Privacy Commissioner. How many people have complained about their laptop and electronic device searches through that mechanism? How many people have complained in the course of recourse directorate reviews? Also, even getting a number of narrative reports written by CBSA officers...they are a treasure trove of information as to what happened with respect to a particular incident at the border. You will find information in there.

● (1705)

Hon. Steven Blaney: Do you have any recommendations, examples, on what good oversight would look like? We have other organizations that have oversight mechanisms. Some have said we could regroup or use the existing oversight mechanism that we have.

Ms. Cyndee Todgham Cherniak: One option would be that if an officer would like to search a cellphone, he would need to fill out a piece of paper and ask a supervisor to sign off. There would be a report written, not only about the decision to search an electronic device but what they are looking for on that device.

Let's just say that they are looking for the invoice concerning a particular camera that they think was purchased outside Canada. You could narrow what they are looking for. They can't go on a fishing expedition if, in that form, they need to state specifically what it is they would like to search. If what they want to search is, say, a lawyer's laptop, we would be able to stop them from looking for information about a particular client.

Hon. Steven Blaney: Isn't the issue that CBSA is overlooking its own activity? Should there not be an independent oversight body that would review those mechanisms after a certain level of review, as you've explained?

Ms. Cyndee Todgham Cherniak: I think it would be a great idea to have someone other than the CBSA looking at the CBSA activities, especially in connection with electronic device searches and solicitor-client privilege at the border. There needs to be someone other the CBSA policing their own.

Hon. Steven Blaney: Please, Mr. Klein.

Mr. Kris Klein: The problem with the Privacy Commissioner being the only body that really oversees CBSA right now is that under the Privacy Act there are a few shortfalls. One is that it's complaint-driven, so somebody has to actually file a complaint. The other thing is that we have a really low standard of the Privacy Act that allows government institutions like the CBSA to collect personal information on a very low standard. Right now the law says that the CBSA can collect any information so long as it relates to an operating program or activity. We heard the Privacy Commissioner say many times that this needs to be augmented. We need the test to be, is it necessary for an operating program or activity? I think if you increase the commissioner's powers, and if you fix the threshold by which government institutions can collect personal information, you're moving in the right direction.

Hon. Steven Blaney: Thank you.

Mr. Geist.

Dr. Michael Geist: I just want to highlight the problem with a complaint-driven process in an environment when it's largely a black box to most individual users...about the availability of a complaint process as well as what the proper guidelines are. The concern, I would argue, from an individual's perspective, knowing that there's an ongoing record, is the prospect of being red flagged as someone who has launched a complaint. The risk inherent in sticking yourself out and saying you're going to launch a complaint is that even if it's well-founded, what are the repercussions longer term?

There's a reason in access to information requests. We ensure that there's anonymity for the requester so that there isn't that ability to identify. Any system where there is oversight that is at least in some way reliant upon complaints—and we've already heard about why a complaint-driven process raises some challenges—has to ensure that there is anonymity for the person launching the complaint because without that, I suspect most people will say the risk of repercussions longer term outweighs any benefits they might get from filing the complaint in the first place.

● (1710)

The Chair: Thank you, MP Blaney.

MP Trudel, for seven minutes.

[*Translation*]

Ms. Karine Trudel: Thank you, Mr. Chair.

Thank you very much for your presentations. They were very interesting and instructive.

My question is for you all, and deals with complaints over searches. I read a Supreme Court of Canada report about it.

How can we strike a balance between the provisions of the Canadian Charter of Rights and Freedoms, our privacy and our freedom as individuals, on the one hand, and our security, on the other?

There has been a lot of talk about the fact that we have rights. Given all that, how can we keep things in balance?

I would like to hear your opinion and your ideas about it.

[*English*]

Mr. David Fraser: I'm happy to start.

In the last number of years we've clearly have had a recognition from the Supreme Court of Canada of the very high value of privacy that is existent in these devices. They are at the very high end of the scale. You can get a search warrant to search a house, and if it contains a computer, you need an extra search warrant to go into that computer. We actually have a recent case from the Supreme Court of Canada which recognized that there are circumstances where maybe that can be pierced in a little way, and that's the search incident to arrest. That's where, by analogy to the kind of security imperatives at the border, you have officer safety issues, you have the destruction of evidence issues, things like that, and the Supreme Court of Canada said ordinarily that you can never get into this thing without a warrant, but in a search incident to arrest we'll let you in there, but only in a very careful, very controlled way.

That may be in fact the middle ground, the documenting of exactly why you're doing it, what you're doing, and how you're doing it. I think part of that also is it's too easy for the CBSA to get into these phones. They have their policies and they have their procedures, but according to the law, as they seem to understand it, a CBSA officer can go looking through a young woman's phone just because she came from Cuba and there may be bikini pictures on it. There is no threshold in the law, as they understand it, to allow them to do that. There needs to be a balance, but it certainly doesn't need to be down here. It needs to be higher, up here.

Dr. Michael Geist: I would start my response by noting—I think it was Kris that noted—that the courts often say that you have no reasonable expectation of privacy. I think part of the problem here is that, if we are reliant on a reasonable expectation of privacy, but many people have in a sense been taught that you should not expect any privacy when you're crossing a border—I don't think that's the right thing to have been taught. However, from an experiential perspective, that is how many people regard that experience. Then it is a bit of a self-fulfilling prophecy, if we're reliant on a reasonable expectation of privacy, but people don't expect any, well then they say, “Sorry, you got exactly what you expected.”

From my perspective, one of the starting points for solving this issue is to leave out the privacy side and let's establish reasonable expectations about what people will encounter when they cross the border. Part of that depends upon far better disclosure and information. We've already seen, in some of the questions here where there is confusion, even after you've heard from the CBSA or other officials about what the policy happens to be.

If you're getting the actual officials in here and questioning them and you're still not sure about what is actually taking place, Canadians can hardly be blamed for not having any real understanding about what the standards are, much less the fact...the idea that we ought to be separating what Canadian officials are doing and what U.S. officials are doing. When we have U.S. officials on Canadian soil, many people struggle to distinguish between what's taking place because it's all happening here, at the Ottawa airport, or at Pearson, or wherever it happens to be, even if the officials come from different places.

Even before we say let's set out and fix the law, we have to begin, I think, to establish reasonable expectations for people, which must surely come from far better disclosure and clarity about what is permitted and what is not. I think that will allow for a much more robust debate to ensure that people do sleep well at night, when it comes to the kinds of standards that we have about protecting our borders, but also sleep well at night knowing that the next morning, when they're going to the airport, they're not going to be subject to an invasive search that seems inappropriate.

● (1715)

[*Translation*]

Ms. Karine Trudel: Earlier, you talked about Bill C-21. I believe that the bill will be voted on this evening in the House. You talked about preclearance, broader powers, and the need to establish parameters.

Can you give us more details about it and tell us what you think of it?

[*English*]

Mr. David Fraser: Sorry. Are you referring to Bill C-21 or Bill C-23, the preclearance act?

[*Translation*]

Ms. Karine Trudel: I am talking about Bill C-21.

[*English*]

Mr. David Fraser: If you're voting on it, there may not be a whole lot that we can offer.

The element that I focused on in the comments and also in the submission relates to what seemed to be an expansion of CBSA and general Canadian government powers with respect to Canadians who were exiting the country. CBSA has traditionally been focused on keeping threats out of Canada and people who aren't authorized to be here and otherwise.

There seems to be an additional spreading of their attention to Canadians who are otherwise engaged in lawful activity, which can include leaving the country. The same powers that they're looking at, which they already have with respect to people and goods entering the country, they're looking to have for goods that are leaving. We don't see that that's necessarily proportional.

It's one thing to keep the theoretical bad guys out of Canada and CBSA is on the front lines of that. However, regarding the threat of things leaving Canada, well, you can unlawfully export a whole bunch of things, which I don't think requires the same commensurate power. There needs to be a proportionality. They shouldn't have the ability to pull any Canadian standing in a departure lounge into the back of the airport and interrogate them, where if they don't answer a question, they can be charged with obstruction. That seems to me to be a disproportionate response.

[*Translation*]

Ms. Karine Trudel: Thank you very much.

[*English*]

The Chair: Thank you.

Now we'll go to Mr. Fragiskatos.

Mr. Peter Fragiskatos (London North Centre, Lib.): I'm not a member of this committee. I'm sitting in for a colleague today but I'm extremely interested in the topic, not just as an individual MP, but certainly I know constituents have raised matters of privacy.

I am looking at a report here. I'll read from it. It says on the CBSA and their powers with respect to devices:

> The agency's policy states that personal devices should only be searched when officials have reason to believe a device will contain "evidence of contraventions" or proof you have violated a law through files or information "known or suspected to exist" on your phone.

I have two questions with respect to evidence of contraventions.

I'm going to assume that relates to evidence of contraventions of the Customs Act. Mr. Fraser, you talked about an example from Cuba. Could you go into that because I wonder, is there a clear list of contraventions that are being followed here or examples of contraventions or is it simply up to a guess on the part of the CBSA officer? Also, when it comes to information, files for example that are known or suspected to exist, what does "suspected" mean according to what you've been able to gather?

Mr. David Fraser: I think suspected is just simply that: they believe it might exist.

The issue is at its core. CBSA has a policy and says these are the circumstances under which they will inspect devices and open them up and demand passwords. It sets the bar here according to their policy. I've heard from front-line CBSA folks who say that's more of a suggestion or a guidance than an actual policy. But the law that they rely on they say is down here at the bottom. Everything that's in the middle, everything that protects the privacy of Canadians and makes an intrusion of privacy proportionate, is based entirely on a policy that is followed maybe most of the time; we'll assume everybody's good faith.

The reality is that you cannot make something constitutional by a policy. They could put it in a regulation, which would then have the force of law, but they have not. It is a piece of paper that could be disregarded at any time with very little recourse. I think that's a significant problem with the entire thing as it's set out.

● (1720)

Mr. Peter Fragiskatos: You commented just now on what's suspected to exist and you put out an explanation, but when it comes to proof that one has violated a law through files or information that might be on one's phone, does the word "suspected" relate to the fact that they think it might be on the phone but they can't find it? Is that what that means?

Mr. David Fraser: I think having suspicion would come into play in a number of different directions. They suspect it exists. They suspect it relates to wrongdoing. They suspect they might be able to find it. The example they gave is you crossed the border or you came into an airport and you had a very expensive purse and they think it's new and they think they might find the receipt for it on your phone.

I would assume what would inform their suspicion is whether you appear to be a savvy enough person to organize your receipts electronically. Would that exist? Is it a Nokia from 20 years ago or is it an iPhone from now? There are probably a whole bunch of variables that you could never necessarily put into a great flow chart, but these questions are dealt with by law enforcement across the country on a daily basis not just at the border.

I think there are ways these can be arrived at. One thing that's also worth noting just in a general context, is the courts have also said the border is not in a no-charter zone. They have said you have a reduced expectation of privacy, but the charter still applies at the border.

Mr. Peter Fragiskatos: I think my dad owns a 20-year-old Nokia. He's savvy but not in a negative sense.

Mr. Geist, maybe this is an unfair question because you've written so much on a range of topics. When it comes to the privacy of Canadians at airports and borders, is there one specific major concern you have right now? Once you highlight it, I wonder if you could point to a country that has dealt with this issue from a privacy perspective through legislation.

Dr. Michael Geist: That's a good question. I'm not sure if it's unfair, but it's a good one.

I think—and it has been highlighted by a lot of your witnesses—that the move to the electronic and digital world has meant that the scope of a search is not the scope of a search from a decade ago. If we are looking at it purely from where the law is at, and the reality of the implications from searches today, quite clearly the concern arises that, once you shift from the physical belongings in my bag, whether that's a new handbag or some other sort of thing that is there, into, in a sense, the cloud—although we did hear the notion that they are not looking in the cloud but strictly for what's on the device, so much gets stored on these devices—that's where I think there has to be a bit of catch-up.

For me, a close second—I guess it's a theme because I've raised it now a couple of times—is the lack of clarity and the uncertainty associated with what takes place. This is, for me, a really serious concern. I didn't mention it, but I think in some ways it's one of the reasons this issue resonates with people. Literally, I think every person will have a story. I can recall, for myself, immediately after the Trump executive order, I was crossing a land border with my son to go to some basketball games in March. As we were going there, there was a lot of uncertainty. What exactly are they going to ask? Are they going to just let us through, or are they going to want to see phones or devices, or question whether I am permitted to go with my son across the border and whether there is a letter from my wife? What other information are they going to look for? There is no place where you can get that. I crossed, and they waved us through immediately. I'm a lucky white guy, as it turns out.

The reality is that, for me, it's usually not that big a deal, but for an awful lot of people, depending on where they were born, the colour of their skin, or the background they have, this is an issue that keeps them up many nights and raises enormous fears. Finding ways to address that, and, I would argue, address it on both sides of the border.... I don't think we can solely say, let's fix the Canadian side of the issue, while recognizing that for millions of Canadians, the issue will still remain. Especially when we are in the midst of active negotiations with the United States about NAFTA, that surely is one of the places where there is an opportunity to try to craft some of these solutions.

As for the question of who's getting it right, I think everybody is struggling with these issues, and everybody's circumstances are different, in terms of the security imperative and the like, which makes it difficult to identify precisely the right place to land.

● (1725)

Mr. Peter Fragiskatos: Thank you very much.

The Chair: Thank you, Mr. Fragiskatos.

Mr. Gourde, you have the last five minutes. It might be down to four minutes.

[*Translation*]

Mr. Jacques Gourde: Thank you, Mr. Chair.

You emphasized that, in the NAFTA negotiations, it is not always easy to find common solutions with all the countries.

In terms of the security of electronic devices and the information that may be extracted from them, do the countries tend to favour a common approach or does each one prefer its own formula?

[*English*]

Dr. Michael Geist: This is obviously a commonality among many countries, especially attempts to facilitate border crossing and make it easier. One of the problems with those attempts to facilitate and make life easier is that it comes with the provision of a massive amount of information, which then gets widely shared. The vision is, let's make it easier for people to travel across borders, but the price of doing so becomes passenger lists, other sorts of information, or biometric data, as you provide in a NEXUS context.

There has been a large price, it seems to me, in terms of some of the things that people have to surrender as part of that. Perhaps other colleagues on the panel have their own experience or knowledge, but I think we are seeing many countries grapple with some of the same kinds of questions.

One thing, though, that distinguishes our country from pretty much all others, save, I suppose, Mexico, is that our border is with the United States, or at least our most commonly traversed border is with the United States. Given what we are seeing take place in the United States, it really is unavoidable to begin to look at those issues, especially in the way that we have tried to facilitate some of those border crossings by saying, let's do pre-clearance, and, in fact, let's facilitate as much pre-clearance as possible.

[*Translation*]

Mr. Jacques Gourde: My impression is that giving the password to an electronic device to a customs officer is basically giving the officer permission to search that device.

In terms of security, I feel that the technology that countries have today allows them to search our personal information anyway. In reality, they are just asking for permission pro forma. If they actually have any real doubt, they are going to find a way to search the information about us, whether it is in the cloud or elsewhere.

[*English*]

Dr. Michael Geist: Countries do search. Whether or not they ought to be searching is a completely different question. Whether or not there are the appropriate oversight mechanisms, safeguards, and protections when they do conduct those searches is also a different question.

Can the NSA engage in widespread surveillance, and can some of our own agencies assist in that? Technically speaking, we know the answer to that. They can, and we know that they do.

I don't think that answers the legal question, and I don't think it answers the moral question either as to whether or not they ought to be doing that. Even if you conclude that they ought to be doing it in appropriate circumstances, whether or not we have the appropriate safeguards and oversight as part of those searches....

Hon. Steven Blaney: Mr. Fraser, I have a question on your second recommendation.

With respect to the preclearance act, why can someone who comes to the border then withdraw? If a person doesn't want to cross the border when the person is at the border, why do you feel there is a reason the person can turn around?

The Chair: Make it a short answer, please.

Mr. David Fraser: The situation is that people can currently withdraw. The change in the legislation is going to allow the detention of that person and an interrogation in order to determine why they did that, which actually defeats the purpose of the withdrawal in the first place.

Hon. Steven Blaney: Are you saying that we should maintain the same right of withdrawal we have now?

Mr. David Fraser: Yes.

Hon. Steven Blaney: Before and after the preclearance act?

Mr. David Fraser: Yes.

Hon. Steven Blaney: Thank you.

The Chair: Thanks to everybody who came today to our committee. We appreciate your testimonies.

The meeting is adjourned.