HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 066 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Monday, September 18, 2017

Standing Committee on Access to Information, Privacy and Ethics

Monday, September 18, 2017

● (1555)

[*English*]

The Vice-Chair (Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.)): Welcome back, everyone. Today we have our 66th meeting of the Standing Committee on Access to Information, Privacy and Ethics. We're continuing our study with respect to the protection of Canadians' privacy at the border and in the United States.

To that end, we're joined today by the Office of the Privacy Commissioner of Canada, their representation including Mr. Therrien, the Privacy Commissioner; Ms. Ives, the acting director general of audit and review; and Ms. Kosseim, senior general counsel and director general of legal services, policy research and technology analysis branch.

The floor is yours.

Mr. Daniel Therrien (Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada): Thank you very much, Mr. Chair, for the invitation to appear before you today on your study of the border.

Privacy rights and the border must be considered in context, and an important element of context is that trade is, of course, important to Canada. This means that smart controls for border goods and data, as they move across borders, are required.

One topic of discussion flagged for your current study relates to screening and searches by Canadian border services officers. As you know, the powers of border officers are quite broad. They may question travellers, collect biometric information for identification purposes, as well as examine, search, or detain any goods.

As for searches of the person, they may also conduct pat-down searches and frisks, take X-rays or body scans, and they may even demand strip searches or body cavity examinations. All searches of persons require reasonable grounds to suspect some legal contravention, particularly the concealment of goods or of anything that would present a danger to human life or safety.

For their part, electronic devices have historically been considered as goods by the CBSA. Paragraphs 99(1)(a) and (c) of the Customs Act allow for examination, opening, and taking samples of goods without grounds. These provisions apply to materials both entering and leaving Canada. In addition, under existing charter jurisprudence, greater latitude is given to state authorities at the border to enforce sovereignty and territorial integrity and to regulate immigration.

At the same time, though, the Supreme Court has found in many other contexts that searching of electronic devices is extremely intrusive. Therefore, while the law is not settled, I think it is clear that Canadian courts would find that groundless searches of phones, of cellular devices, were unconstitutional even at the border.

The idea that electronic devices should be considered as mere goods and therefore be subject to border searches without legal grounds is clearly outdated and does not reflect the realities of modern technology. This may well be why Canada's policy is more nuanced than what the Customs Act may allow.

Under CBSA policy, specific grounds need to be satisfied, namely that “evidence of contraventions may be found on the digital device or media”. I think that policy is wise, but it should in my view be elevated to a rule of law in the near future.

Another border issue of note concerns Bill C-23, which is now before the Senate. Bill C-23, the pre-clearance act, 2016, would implement the 2015 agreement on land, rail, marine, and air transport pre-clearance between the Government of Canada and the Government of the United States. This would provide for pre-clearance activities on the part of the Canadian and U.S. customs officials to take place at various points of entry on both sides of the border.

I've raised concerns about U.S. announcements to search the electronic devices of any and all aliens who seek to enter the U.S. These searches will be at their discretion and without specific legal grounds other than generally to protect homeland security.

Bill C-23 establishes that U.S. pre-clearance officers in Canada are subject to Canadian law as they perform their duties or exercise any powers. The Canadian government reminds us that this would include the Canadian Charter of Rights and Freedoms, the Canadian Bill of Rights, and the Canadian Human Rights Act. However, these protections are somewhat hollow, as they would be severely limited by the principle of state immunity, meaning that they could not be enforced in a court of law.

It should be noted that under Bill C-23, searches of persons, including relatively non-intrusive pat-down searches, require "reasonable grounds to suspect" in order to be carried out by U.S. officers in Canada. In my view, searches of electronic devices can be much more intrusive than these frisk searches.

● (1600)

As I recommended in the context of the study of Bill C-23, border searches of electronic devices should require reasonable grounds to suspect, the same threshold that applies to searches of persons.

[*Translation*]

This past spring, I informed you of my correspondence with the three appropriate ministers regarding the executive orders of the new U.S. administration, issued earlier this year. Measures like these clearly have a material effect on the privacy of many citizens, given the scale of tourism and business travel to the United States.

One order would specifically exclude non-U.S. citizens and lawful permanent residents from certain privacy protections.

Upon review, I have concluded that, while Canadians have some privacy protection in the United States, that protection is fragile because it relies primarily on commitments or administrative agreements that do not have the force of law, for instance the Five-Eyes Agreement and the Beyond the Border Agreement with the United States.

I have therefore called upon our government to ask their U.S. counterparts to strengthen privacy protections for Canadians. This could be done, for example, by adding Canada to the list of designated countries under the U.S. Judicial Redress Act, which would extend some of the protections conferred by the U.S. Privacy Act to Canadians, as they are in place for citizens of several European countries.

We have also asked the government for assurances that the protection afforded by Canada-U.S. administrative agreements will continue despite the order and to be advised of any changes that may adversely affect the privacy of Canadians. We understand that the findings have now been compiled and a response is forthcoming.

Let us turn now to the information-sharing agreements with the United States.

Generally speaking, we have spent considerable time on border issues and information-sharing in the past several years, in particular, the Beyond the Border initiatives with the United States. To date, we have provided feedback on close to fifty separate privacy impact assessments (PIAs) on just these programs alone. Through these exchanges, we have made a series of recommendations to the CBSA and various other federal departments implicated in expanding information exchange and other border-related processes.

Overall, we have been pleased with the level of consultation and the improved quality of privacy analysis undertaken by agencies involved with border security.

That said, we still have concerns over issues such as retention periods applicable to data collected from travellers and the risk that data collected for border purposes is then used for secondary purposes.

Both of these issues were found to be problematic from the point of view of European law, in a recent judgment of the European Court of Justice on the Canada-EU API/PNR Agreement.

In closing, as people, goods and data move across borders more frequently, it is important that Parliament ensures that we have the appropriate rules in place to respect individuals' privacy. The importance of the rules has been recognized historically in relation to the search for persons. In my opinion, it is time to extend these safeguards to electronic devices.

Thank you for inviting me and I look forward to your questions.

● (1605)

[*English*]

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thanks very much.

We'll begin the seven-minute round of questions with Mr. Saini.

Mr. Raj Saini (Kitchener Centre, Lib.): Good afternoon, Mr. Therrien, and to your colleagues, thank you very much for coming. I was joking with you. I think you're almost a permanent member of this committee because you're here at least once month. I hope you enjoyed the summer like we did.

Mr. Daniel Therrien: I did.

Mr. Raj Saini: Now that we're here, I want to ask a bit of a technical question because certain things happened in the spring. The FCC changed some of the Internet provider rules, and Trump's executive order was done at the same time. Therefore, now you may have the potential impact of a Canadian going to the American border, and he may be asked for a password of his device—that's one issue—so now his privacy is not protected. However, the other thing is that now when he gets to a certain point, he may have his phone or something connected to their Internet, so his information may be sold according to the FCC rules.

Can you give us an overview of what your opinion of this is, and also what advice you would have? How do you think this is going to affect us domestically here?

Mr. Daniel Therrien: It's quite a broad-ranging question.

Mr. Raj Saini: You have seven minutes.

Voices: Oh, oh!

Mr. Daniel Therrien: Of course, the first thing to say is that states are sovereign, including the United States of America, so in the comments that I've made in my opening remarks, I call on the Canadian government to take certain measures to protect the privacy of Canadians, first and foremost, in devising appropriate laws that protect the very sensitive information found in electronic devices—that's Canadian domestic law—and to the extent possible, in the pre-clearance agreement.

But at some point, a Canadian who wants to visit the United States either for tourism, business, or other reasons will come up against U. S. state authorities, and the U.S. is free to adopt the rules that are in their interest in order to protect their safety. That, apparently, means in part that U.S. border officials.... If you just set aside pre-clearance, if a Canadian wants to go to the United States and comes across a border officer, either inland at the border or at a U.S. airport, that person may be required to provide the password to their cellphone.

I don't think that is protective of privacy, but it is within the powers of the U.S. government to impose that rule. We may come into what that means in terms of a prudent approach by a Canadian who will face that situation, but you're now talking about U.S. laws and practices. The U.S. is competent and has the authority to impose these rules. I don't think they're good rules, but these are the rules that apparently will be imposed on travellers.

You're bringing in the private sector angle with your reference to the FCC changes and whether information collected by the U.S. government could be sold. I haven't analyzed this in any great detail. Certainly, following the executive order of President Trump that limited, if not eliminated, privacy protection for non-Americans, we were seized with, of course, concerns by Canadians. We looked at the situation of whether Canadians are protected. There are no laws to protect Canadians, but there are a number of administrative agreements that, until rescinded, do provide some protections. Among these administrative protections is an order made by then-president Obama that provides similar protections to non-Americans in regard to the activities of the NSA, particularly what the U.S. government does with information intercepted in the name of foreign intelligence.

I'm giving you the *grande ligne* of the rules that are applicable. There are still remaining administrative protections in the U.S. Of course, they are administrative protections and they could be rescinded tomorrow by the U.S. administration, but there are still, at this point, a number of administrative protections for Canadian citizens.

● (1610)

Mr. Raj Saini: I have one final question, and I'll make it a little bit easier.

We know that the GDPR rules are going to be coming into effect in May 2018. We also know that right now the United States and Europe have a privacy shield, which we don't have, and eventually the European Union is going to ask that everybody rise to their level in terms of the regulations that they will have.

Do you think it would be prudent or probably easier and more facile if the United States, the European Union, and Canada could somehow come to one standard, as opposed to the United States and Europe having one standard, and Canadians not having any protection because of the executive order?

Mr. Daniel Therrien: It would certainly be easier, but it is a well-known fact that there are important differences of approach between the United States and Europe with respect to privacy, so I don't think that this will happen any time soon, which puts Canada in a difficult position, obviously.

I've asked that certain legal protections be given to Canadians. For instance, asking the U.S. government to add Canada to a list of countries to which protection is given under the Judicial Redress Act would not be the whole way to having a tripartite regime, but there are steps. My point is that there may be steps along the way stopping short of having a tripartite privacy protection regime as between the EU, the U.S., and Canada.

Mr. Raj Saini: Can you quickly give an example of some countries that are on the judicial redress list?

Mr. Daniel Therrien: A good number of European countries, more than 20, are on that list, essentially because of pressures put on the United States by European states along the lines of the conversations they are having with the U.S. that led to the privacy shield. All these issues are related, and it is not a benevolent act by the U.S. to have designated certain European states on that list. It's because pressure was put to bear on the U.S. by these European states. That could be an approach for Canada.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thanks very much.

With that, we go to our second seven-minute round of questions.

Mr. Kent, welcome to the committee.

Hon. Peter Kent (Thornhill, CPC): Thank you very much, Chair. It's a pleasure to be with you.

Thank you very much, Commissioner, Ms. Kosseim, and Ms. Ives, for joining us today.

As we all know, as most Canadians know, the manner of screening and searches varies very much from screening officer to screening officer, location to location, air pre-clearance as opposed to ground and maritime pre-clearance.

Do you have statistics categorizing complaints from the three different sorts of clearance in the questioning, the procedures, say, at a land border as opposed to pre-clearance at Pearson International, or for maritime arrivals and departures of tourist vessels?

Mr. Daniel Therrien: I can undertake to give you these numbers. I don't have them right now, but we don't have a very large number of complaints on these issues. The announcements of a few months ago about new U.S. government practices with respect to cellular devices led to a handful of complaints. Before that we had fewer than 10 complaints on border issues altogether. Our trends will not be based on very many complaints.

● (1615)

Hon. Peter Kent: Most of them would be anecdotal or media reports of complaints.

Mr. Daniel Therrien: Yes.

Hon. Peter Kent: Very often, when we as parliamentarians travel to certain countries around the world we're advised to leave our personal devices at home and to take what is euphemistically called a “burner”, with only as much as information as we would want to share with individuals in these particular countries.

Would you advise, until we have a clearer picture of exactly how this will happen, that perhaps Canadians should think about what they have in their devices before they travel, and where prudent, leave them at home and carry a burner?

Mr. Daniel Therrien: I would certainly advise Canadians to limit the number of devices they bring to the U.S. and to review and limit the information that is found on the devices they're bringing with them to the United States. I think it would be prudent to see whether you could leave in Canada on local devices, your home computer and whatnot, information that you want to keep and that you may not need in the United States.

Another potential measure would be if professionally you need information in the United States, say information protected by solicitor-client privilege or other legal privileges in Canada, and you don't want it to be reviewed by U.S. customs officers, you may want to put it on a secure part of the cloud, for instance, so that it's retrievable once you are in the United States and you can access it then. In short, think hard about what kind of information you want to bring with you in your electronic devices as you cross the border because we have heard that information can be required by U.S. customs officers. It's prudent to act accordingly.

Hon. Peter Kent: We as parliamentarians have different levels of security on our devices besides the thumbprint or the password to get into the general area. Would you advise again at the same time there is as much vulnerability to parliamentarians or private business people as to private citizens who may have secondary levels of security or even encryption, and they too could be required or asked to open those other levels?

Mr. Daniel Therrien: The announcement made by the U.S. administration is that they can require information found on your devices for no legal grounds other than an understandable desire to protect homeland security, but with no legal grounds whatsoever. That applies to everyone and anyone, and it applies regardless of the security measures you have on your device. They say, “If you are to enter the United States, we can require that you give us your password or whatever security mechanism exists between us, the border officials, and the information we want to look at.”

Hon. Peter Kent: You referenced the data retention period questions and the judgment of the European Court of Justice. Did the European Court of Justice look at data retention generally, or did they look at the difference between GPS locator records, phone number records, or text records?

Mr. Daniel Therrien: The European court looked at a very specific program, a draft agreement between Canada and the EU having to do with the transfer of certain types of passenger information between Canada and the European Union. It dealt specifically with that information, although lessons can be learned about other border control programs. The judgment itself had to do with that specific program.

Hon. Peter Kent: I see.

Finally, I have one very short question. You said the government has assured you that a response is forthcoming to your request for assurances. What would you understand is coming?

● (1620)

Mr. Daniel Therrien: They tell me that the U.S. has provided them with some information and that they will send it to our office shortly.

Hon. Peter Kent: Thank you.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): With that, we move to Mr. Cullen.

Mr. Nathan Cullen (Skeena—Bulkley Valley, NDP): Thank you, Chair.

It's nice to see you again, as well, Mr. Therrien.

I am coming at this conversation from a layperson's point of view, which I think is actually an advantage in this one. For the broader Canadian public, the travelling public looking to get to the U.S., it's about setting expectations. What you've told us here today is that the expectation Canadians should have is that it is entirely foreseeable and quite legal for a U.S. customs officer to insist to receive all the information on any electronic device they have coming through the border.

Mr. Daniel Therrien: As a matter of law, yes.

Mr. Nathan Cullen: Right, so no Canadian should cross the border with a phone, a laptop, or an iPad without having great comfort with a U.S. customs official looking through every bit of it.

Mr. Daniel Therrien: I say yes, as a matter of law. Of course, the border could not be managed if everyone were to be searched, but as a matter of law, yes.

Mr. Nathan Cullen: Okay. As a matter of law.... Just for the political fallout, I could never imagine this happening, but imagine our capable trade minister, or a deputy or an official, crossing the U. S. border ready to negotiate NAFTA, with a laptop in hand, and on that laptop is our playbook, or an assistant deputy minister going down to negotiate an important trade agreement. Under current law, with the broad range of powers sitting at the border agencies, that laptop and the plan, the information, could be exposed.

Mr. Daniel Therrien: It's subject to diplomatic relations.

Mr. Nathan Cullen: But not subject to the law.... Diplomatic relations, sure. There might be an outcry, but in terms of legal ground, it's totally solid.

Mr. Daniel Therrien: Yes.

Mr. Nathan Cullen: Okay.

I was looking at the designated countries list, the list where Americans have said, “We have designated you as secure enough to allow you in and to allow you the same protections under the U.S. privacy law.” Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Italy, Latvia, Lithuania, Luxembourg—all these countries have been able to establish protection for their citizens under U.S. privacy law, whereas Canada either has not sought that protection or has not been able to earn that protection yet. Is that right?

Mr. Daniel Therrien: The basis on which the U.S. has designated countries on that list has less to do with the security of information for Americans. Actually, it's the other way around. Europeans, of course, have strong privacy laws, and they have put pressure on the U.S. government, saying, "You should protect the information of our citizens—Poland, etc.—in an adequate way; otherwise, we will not share information with you."

Mr. Nathan Cullen: Again, back to my question. Has Canada either not asked for similar protections for Canadian citizens, or asked and not received that protection?

Mr. Daniel Therrien: I do not know whether the Canadian government has asked, but certainly Canada could ask.

Mr. Nathan Cullen: Certainly if Estonia was able to ask for and be granted that protection for Estonians travelling to America, I don't think a trade war with Estonia was what brought Americans over to the side. Clearly as their largest trading partner, one would assume we'd have more influence in these types of conversations.

Mr. Daniel Therrien: The fact that we are an important trade partner for the U.S. is obviously a relevant consideration.

Mr. Nathan Cullen: Beyond our travelling public, our business travellers, folks that have many enterprises in the United States.... Okay. That's interesting.

You said earlier, in response to my colleague's question, that Canadians should limit the number of devices they bring in. That is your office's official recommendation for the travelling public: don't bring everything you have, and what you bring.... Maybe we have to resort to such cloak and dagger items as burner phones, but normally Canadians may acquire a phone like that simply for cheaper cell rates if they're travelling and working in the U.S.

On a privacy level, is it your recommendation that I should not bring my work phone when I travel in the U.S.?

Mr. Daniel Therrien: It starts with what kind of risk tolerance you have about your information being looked at by U.S. customs officers. There's a personal assessment to be made. For instance, if there's privileged information on your device, then obviously you have a higher responsibility to protect that information. My point is to think about what you're exposing your information to and limit the amount of information that you bring to the U.S., because it may be acquired by customs officers.

● (1625)

Mr. Nathan Cullen: Because it gets shared. It doesn't stop with the customs officer. With the way the American security regime works, high sharing is the.... I'm just remembering a constituent—

Mr. Daniel Therrien: It could be shared.

Mr. Nathan Cullen: A constituent of mine got denied at the border because personal information was taken from their phone that showed they had a prescription for heart medication, and the border official said, "We don't want you coming here and having a heart attack. You can't come in." I thought this was a strange invasion of one's privacy while seeking to simply be on vacation in another country. That information was then shared with a U.S. health agency.

Another constituent one riding over was denied because they were showing that one of their prescriptions that the officers were able to pull up was a prescription for treating AIDS, and the American border official said they couldn't come in because of that.

Mr. Daniel Therrien: It's certainly possible.

We have received a complaint some time ago from an individual. This had nothing to do with electronic devices, but somebody was refused admission to the U.S. based on the fact that they had called 911 in Canada during an event of trauma. The person was considering suicide, and that was the reason she was refused admission to the United States. It's a bit similar to your example about a health condition that can lead to the refusal of admission to the United States based on such information.

Mr. Nathan Cullen: I have one last question. Does the investigation always have to be physical? I'm not a technologist. Is the border agency able to retrieve data off phones at a distance, once I cross over? We had the spy issue with the Toronto Pearson Airport where phone calls and receptions back and forth were being monitored.

Does it always have to be a physical intervention, or can it be otherwise? Do we know?

Mr. Daniel Therrien: If it's not physical, you're now into interception of communication territory, which has different rules.

Mr. Nathan Cullen: Thank you.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thanks very much, Mr. Cullen.

With that, our final seven minutes goes to Mr. Long.

Mr. Wayne Long (Saint John—Rothesay, Lib.): Thank you, Mr. Chair, and welcome to all of the new members on our committee. It's great to have some new faces.

Mr. Nathan Cullen: Were you tired of the old ones?

Mr. Wayne Long: Well, I didn't say that.

Again, Mr. Commissioner, thank you so much for coming. You are a regular and we appreciate your input.

I thought I would start by sharing a story of what I went through not too long ago while crossing the border. My riding is Saint John-Rothesay, and I'm an hour from the Calais border. We went across, and we were asked to pull in. We went inside to talk with the customs agents, and I was to accompany the agents back to the car. We were told to put all of our phones in the car and open the phones up. Then I left. We sat inside for a better part of 30 to 45 minutes. It was me, a friend, my son, and one other person, and we waited. Eventually, they came back and said we were all good. We went back to the car, and the phones were clearly not in the same places as they had been.

Like Mr. Cullen said, obviously it's cause for concern when you cross that border. Respecting that, as you say, they don't have to give you entry into the United States. But I guess, from a Canadian's viewpoint—and, again, I apologize, it's the same line of questioning as Mr. Cullen.

How concerned should Canadians be? As Mr. Cullen said, we cross now with our iPads, laptops, and phones, and in my phone is my banking information and my emails. It's not just text and pictures anymore. It's basically your life history and all your records. On a scale of one to 10, as Canadians, how concerned should we be?

Mr. Daniel Therrien: As you say, these devices contain a lot of sensitive information. We should be very concerned. The law allows U.S. officers to collect anything they essentially want because there are no legal grounds for their actions. To be realistic, I made a distinction with Mr. Cullen about the law and the practice. Customs officers do not have the resources and cannot review the content of the devices of every traveller who comes across the border. That in a sense is an element of context, but as a matter of principle, I think it is right to say these devices contain a lot of very personal information, very sensitive information. When the law, including Canadian law, continues to treat the content of cellular devices as goods, as a cardboard box, as a piece of clothing, it is just not realistic.

● (1630)

Mr. Wayne Long: Fair enough.

On the OPC website, it talks about "Your privacy at airports" and how you say we should have reduced expectations. I read in the same document that information such as name, date of birth, gender, citizenship, travel document data, itinerary, address, ticket payment information, frequent flyer information, baggage, and contact numbers are collected for—obviously—assessing security risks.

Can you comment just on your thoughts? Is it being disposed of in an appropriate way? How long is it stored? Is it stored properly? Is there any expectation there that information that they do take is held? Is there an agreement with us? Is there something where we can come back and say, "Look, you're holding it for a month", or can they hold it forever?

Mr. Daniel Therrien: You're talking about information collected about travellers by Canadian border officials?

Mr. Wayne Long: Yes.

Mr. Daniel Therrien: Retention is obviously an important issue, but I'll start by saying that it is legitimate for Canadian border officers and, for that matter, U.S. border officers to collect some personal information to determine whether the person who wants to be admitted should be admitted. Therefore, I'm not saying that no information should be collected. Some information is absolutely reasonable to make a decision about admission. But if we're within that area of certain pieces of information reasonably linked to the decision to admit, then our concern moves to how long this is retained—you're right to raise that question—and for what purpose it can then be disclosed to other departments.

Mr. Wayne Long: What's acceptable? What is it? Is it six months? Is it a week?

Mr. Daniel Therrien: It depends on what the purpose is for which you're collecting the information. If, for instance, the information is collected to determine the legality of your status in Canada, I think it's fair to keep it until your legal or illegal status is finally determined. It all depends on what purpose the information is being collected for. It's primarily collected for border management reasons, so there's no one answer as to how long. It depends on what the reason is that it's being collected, and if it's a reasonable purpose, how long does the government need it to achieve that purpose?

Mr. Wayne Long: Thank you.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Great.

With that, we will go to Mr. Gourde for five minutes.

[*Translation*]

Mr. Jacques Gourde (Lévis—Lotbinière, CPC): Thank you, Mr. Chair. I am pleased to join your committee.

Thank you to the witnesses for being here.

Mr. Therrien, do you think the frequency of checks of electronic devices at customs is increasing? Are those checks conducted on a random basis only?

Mr. Daniel Therrien: Are you referring to Canada or the United States?

Mr. Jacques Gourde: I am referring to the United States.

Mr. Daniel Therrien: An increase has been noted in the United States. According to the data collected, 5,000 cell phone searches were conducted in 2015 as compared to 25,000 searches in 2016. That is an increase of over 500% from 2015 to 2016. Moreover, according to reliable figures for 2017, there were 5,000 searches in just one month, in February 2017. So there has been an increase.

● (1635)

Mr. Jacques Gourde: Do your statistics indicate whether certain groups are being targeted more than others? Are there more random searches or is it mostly younger people or older people who are targeted?

Mr. Daniel Therrien: The figures are not collected by us so we have not been able to see them. To my knowledge, there is no targeting of specific groups. That would of course be a valid question to ask.

Mr. Jacques Gourde: I think that is a concern for many Canadians.

Do Canadian customs officials do the same thing? Do they check the electronic devices of Americans entering Canada?

Mr. Daniel Therrien: As I said in my introductory remarks, customs officials can do many things under Canadian law. Under Canadian law, cell phones are treated like property. As such they can be searched without cause at this time. That is the statute law.

The policy of the Canadian government and of CBSA is to restrict this legal authority such that the devices in question can be searched only if the Canadian customs official has grounds to suspect something related to an offence.

So the policy is not as permissive as the law, in my opinion, because the government and CBSA sense that the courts would not uphold the use of powers without grounds as the statute law allows.

Mr. Jacques Gourde: If a Canadian complains because their cell phone was searched, resulting in the loss of trade, patent or other information, does that person have any recourse or is that information lost forever?

Mr. Daniel Therrien: Even though the information is gathered and collected by the government pursuant to its powers, that does not give it the right to use the information for unwarranted reasons.

If the government takes possession of certain information, there is clearly a risk, but Canada may not disclose or use that information as it wishes. It would certainly be wrong to disclose trade secrets without the judicial or legal authorization to do so.

Mr. Jacques Gourde: Have any Canadians made complaints in this regard recently?

Mr. Daniel Therrien: We have in fact received a small number of complaints and we are in the process of investigating them. They pertain to cell phone searches by the CBSA.

Mr. Jacques Gourde: If Canadians complain about U.S. customs, is their recourse limited?

Mr. Daniel Therrien: If a Canadian arrives on U.S. territory and seeks entry, there is no recourse.

The Standing Committee on Public Safety and National Security has, however, proposed an amendment to Bill C-23, which is currently before Parliament and would give Canadians in a pre-screening area access to a border management administrative mechanism, if not access to a court. In my opinion, that is not sufficient, but it is an improvement to the original version of the bill.

Mr. Jacques Gourde: Do you think there could be a reciprocal agreement?

[*English*]

The Vice-Chair (Mr. Nathaniel Erskine-Smith): We might have time at the end for more questions.

The next five-minute round goes to Ms. Fortier.

[*Translation*]

Mrs. Mona Fortier (Ottawa—Vanier, Lib.): Thank you very much, Mr. Chair.

Mr. Gourde, I am pleased that you have started asking questions about complaints, because I would also like to know where things stand.

What type of complaints do you receive? I understand you have received a few. How do you determine whether they are valid in the present context? Has a trend emerged from these complaints?

Mr. Daniel Therrien: In recent months or the past year or so, we have received three complaints about these practices. Under the Privacy Act, we have the legal obligation to review each complaint. Not all complaints require the same degree of rigour, but we do have to review them all.

Since there have only been three complaints, it is hard to say if there is a trend. I can say, however, that these are definitely people who have read in the media or in various notices that their devices could be searched by Canadian or U.S. authorities. People are worried about this with good cause and want to make sure that government practices are legal. So they filed complaints with us and we are examining them.

● (1640)

Mrs. Mona Fortier: Under the new bill, do you think you will be able to process the complaints that you might receive from Canadians in the same way? What kinds of complaints are they?

Mr. Daniel Therrien: Are you referring to the Preclearance Act?

Mrs. Mona Fortier: Yes, exactly.

Mr. Daniel Therrien: If a Canadian has their cell or electronic device searched by U.S. customs officials on Canadian soil under this regime, we have no jurisdiction. That is under the jurisdiction of the American authorities, under the agreement between Canada and the United States.

The only mechanism under which a person could address a Canadian is the one proposed by the Standing Committee on Public Safety and National Security in the amendment to the bill that I just mentioned.

Mrs. Mona Fortier: You mentioned the way things work in Europe. Can you think of any best practices that we could use to improve our current proposal?

Mr. Daniel Therrien: Are you talking about border management in Canada rather than on the U.S. side?

Mrs. Mona Fortier: I am wondering whether we could draw on practices from elsewhere to better protect Canadians as regards their electronic devices.

Mr. Daniel Therrien: European law is strict as to overarching principles. We saw this in the judgment by the European Court of Justice regarding the border program. To my knowledge, European law deals with these matters according to broad principles. In general, it allows departments and government to gather information only when it is necessary and commensurate with the objective in question. To my knowledge, there is no specific rule for the application of these broad principles to customs practices. That said, we could make some enquiries in that regard.

As to the extent of border powers, the issue, in my opinion, is that there is extensive jurisprudence in Canada indicating that the expectation of privacy at the border is less than in other situations since the person is seeking entry to another country. I think this principle remains valid. It has, however, been used to severely limit if not eliminate judicial guarantees at the border.

With the advent of electronic devices, we have to ask some questions. Customs officials have the right to conduct certain searches at the border, but should that extend to searching financial records on a person's telephone, information about their intimate relationships, or the person's health, for instance? Asking the question gives you the answer. Canada needs to get with the times and treat these devices as they should be treated legally.

Mrs. Mona Fortier: Thank you.

[*English*]

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thanks very much.

We'll go to Mr. Zimmer for the next five minutes.

Mr. Bob Zimmer (Prince George—Peace River—Northern Rockies, CPC): Thank you. It's good to be part of the committee. I'm one of the newest members here. Thanks for having us. This is such a nice introduction.

Mr. Therrien, we've talked before. We've actually been in committee before. We've talked about access to information, and about hacking, and securing of devices, etc. I guess an eye-opener for us—and I can't recall the exact date you were there—was when we were talking about what we know as the hacker of today. It's not some high school kid who's sitting at home, getting information for fun. It's organized crime that's going after our information. That's what I'm going to base my question on.

What is the height of abusing this specific information you're talking about? What have you seen in terms of the information being used or abused at the border? Have there been links to organized crime? Has it been accessed by organized crime, this information that's being sought? Have you made that link yet?

● (1645)

Mr. Daniel Therrien: I haven't seen cases of this nature, but I'll say this. The essence of what the law currently allows is to collect a lot of information in the name of border safety. The possibility of criminals, hackers, and so on is a relevant consideration. I don't want to exaggerate the nature of the problem, but the more information the government collects, obviously, the more it's at risk of being collected and hacked by people with criminal intent. That, I think, is another reason that government should be careful not to collect information beyond what is necessary, and even if it is necessary, not to retain it beyond the period necessary to keep it. The government is obviously a repository of a lot of very interesting information that is of interest to people with criminal intent.

Mr. Bob Zimmer: Getting back to my question, have you seen examples? Maybe you can't talk about all the examples before a public committee. Have you seen examples of information that has been collected, like the instance Mr. Cullen referenced, where somebody was not allowed into the country because they had a health condition? To call that “abuse” is maybe not the right term, but what is the height of abuse that you've seen from this information that's collected? As Privacy Commissioner, can you give us some examples that you've actually seen of negative outcomes from collecting this information?

Mr. Daniel Therrien: We've not seen many but we've seen some, and when I say some, again, this is not information collected through devices.

The example I have in mind is a public example of a lady whose information was collected by a police service in Canada during a crisis that she was under, a suicide attempt, when she called 911. That information becomes part of police records, and that information is then disclosed to U.S. border authorities in the name of co-operation between the law enforcement bodies of Canada and the U.S. It led to the refusal by U.S. officers, who did not let her in because they felt that she was at risk of either committing suicide or somehow endangering U.S. people.

That was as a result of this 911 call, but the same could happen through the search of an electronic device that would reveal a medical condition, for instance.

Mr. Bob Zimmer: Thank you.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): You have 45 seconds left, if you want.

Mr. Bob Zimmer: I'm good. Thank you.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): We will have more time, looking at the clock, for everyone to get their questions in.

The last five-minute round of questions goes to Mr. Dubourg.

[*Translation*]

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

It is my turn to say hello to the witnesses who are here with us this afternoon.

Mr. Therrien, I would like to hear about the sharing of information with the United States. You said that your Beyond the Border action plan includes various recommendations, although you still have concerns, primarily as to the data retention period. For my part, I am more interested in the other part, that is, the risk that data collected at the border could then be used for other purposes.

First of all, I would like to know what kind of purposes you had in mind when you wrote that. Secondly, I would like to know how we can prevent information from being used for other purposes.

● (1650)

Mr. Daniel Therrien: To put it into context, we are talking about information obtained by the Canadian government at the border being disclosed to other departments for purposes other than border control.

The Canadian government has publicly disclosed its intention to use such information for program integrity, for instance. It also wants to be able to confirm whether a person claiming to be in Canada for residency purposes, which affords them certain social benefits, really is. That is one of the ways the government would like to use the information. There can also be tax reasons, which could lead to information sharing with police forces, for instance. All these purposes are possible. The government has in fact indicated that it intends to use this information for those purposes.

For our part, we are not necessarily saying that these reasons are unacceptable, but we want to see to what extent the various departments receiving information from customs need it for the purposes of their programs. We are not at that stage yet and we are awaiting information from the government in the form of evaluations of privacy factors. We are waiting for the government to provide certain, more detailed information justifying these purposes.

Mr. Emmanuel Dubourg: Very well.

The retention of this information and access to it by departments are becoming quite important since information is shared without the person's knowledge.

There is another consideration. We have to know whether the department receiving the information has a monitoring process to limit employee access to the information.

Mr. Daniel Therrien: Let me give you an example regarding retention periods. When the CBSA first consulted us about some of these programs, it said it wanted to keep the information for 75 years. Those consultations were some time ago. We discussed this with the agency and it then decided to reduce the period to 30 years, in order to be able to identify individuals, and to de-identify the information after 15 years.

There is a dialogue with the departments. We see that they want to keep the data for a very long time. After discussing the matter, we are often able to reduce the retention period, but it is difficult to have a thorough discussion with the departments. Once again, there is no magic number when it comes to retention. The real question is what the departments need the information for and how long they have to keep it to meet their objectives, but it is difficult to have that discussion with them

Mr. Emmanuel Dubourg: Finally, I assume that these departments have a grace period of sorts, so to speak. In the case of taxes, for example, once the reporting period is over, it is not possible to make further corrections or issue a new notice of assessment. In other departments, there must certainly be a period of three, five or ten years ...

[*English*]

The Vice-Chair (Mr. Nathaniel Erskine-Smith): We're beyond the five minutes, so please be brief.

Mr. Daniel Therrien: May I, for a few seconds?

The Vice-Chair (Mr. Nathaniel Erskine-Smith): We're beyond the five minutes, so just keep the answer brief.

[*Translation*]

Mr. Daniel Therrien: All I would say...

It's okay, I've lost track

Voices: Oh, oh!

[*English*]

The Vice-Chair (Mr. Nathaniel Erskine-Smith): That was briefer than expected perhaps.

That concludes the five-minute round. We will have time afterwards, but we'll go to Mr. Cullen for three minutes first.

● (1655)

Mr. Nathan Cullen: Thanks again, Chair.

This has been enlightening. It seems to me that it's almost like the combination of two forces. One is the more vigorous security environment that we've lived in the last 10, 15, 20 years, certainly since 9/11, plus the incredibly powerful and pervasive technology that we have. I'm wondering, from your perception in dealing with Canadians, those who are raising either concerns or formal complaints, if there's a lack of awareness of what it is to experience, as Mr. Long did, the “Leave your phones in the car and we'll just take a peek” thing, with all the information the phone contains—all of those passwords, all of those bank accounts, everything about you.

If a Canadian were to see a customs official going through all of their luggage and taking everything out and looking through it, or going through their home, that would be an obvious invasion of privacy. These are personal things. Why would they be looking through someone's photo albums? Yet we seem not to have caught up to the technology we have and the power someone has when they say, “I need your phone and you need to give me your password.”

I guess this is more of a philosophical question, but is there a latency, a catching up, for Canadians in terms of what it is to cross the border? If we were to receive this designated country status, would that go towards alleviating most, some, or a few of your concerns with respect to that information we're giving over when we cross into the U.S.?

Mr. Daniel Therrien: Definitely it's taking time to catch up to the new security and the technological advances that we've seen in the last few years, so I would say, yes, there's a question of latency—latency in terms of the public's understanding of what they're exposed to. We'll do our best to inform Canadians through the means that we have, but I think it's also a bit unreasonable, unrealistic, to think that individuals will change completely their way of life for these reasons—and in North America there's a lot of travel between Canada and the U.S. Yes, we can inform some people, and some people will change their behaviour and, for instance, not bring as much personal information, but Parliament has a huge role in ensuring that the laws, to the extent that they deal with Canadian officers, protect people so that they are not subject to groundless searches.

Mr. Nathan Cullen: I'm imagining if I or any of my colleagues put a householder out to our constituents, a notice, and said, "If you're travelling to the U.S., here's what the Privacy Commissioner recommends: take few devices, and have the expectation that anything that's on those devices could be turned over, and by law it can be turned over, to an American official" that might seem alarmist to some Canadians. Would you not agree?

Mr. Daniel Therrien: Quite possibly, yes.

Mr. Nathan Cullen: Yet you've advised this to us.

Mr. Daniel Therrien: Yes.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): With that note of optimism, that concludes our round of questions. I have a few questions I'd like to ask and I know Mr. Saini has a couple of questions as well.

Go ahead, Mr. Saini, and then we'll go to Mr. Kent.

Mr. Raj Saini: I just want to comment on a couple of things that you said. I want some clarity on this matter.

You said that, in 2016, there were 25,000 searches of cellular devices in the United States. From what I read in *The New York Times*, there were 383 million arrivals in the United States. That represents 0.0012%. Out of those 25,000, is there any way to differentiate how many were actually Canadian? Are you saying there were 25,000 Canadians? Is that in general, just so we can have an understanding of the numbers?

Mr. Daniel Therrien: We'll confirm later, but I believe this number of 25,000 is the number of searches of electronic devices on non-Americans, but not necessarily Canadians.

Mr. Raj Saini: Therefore, there's no breakdown of the Canadian number in that?

Mr. Daniel Therrien: No.

Mr. Raj Saini: Okay.

The second question I have is for my understanding. This is where I would seek your clarity and wisdom.

From my understanding, the EU-American privacy shield deals with information that is sent from one organization in Europe to another organization in the United States.

Mr. Daniel Therrien: Or vice versa....

Mr. Raj Saini: But it does not, under any circumstances, preclude a U.S. border agent from seeking a search from anybody who is travelling to the United States from those countries.

Mr. Daniel Therrien: Indeed.

● (1700)

Mr. Raj Saini: We're talking about two different things here, right?

Mr. Daniel Therrien: It does not change the U.S. law in the respect that you're mentioning. A U.S. border officer could ask a European to give the password to the content of their electronic device. The agreements between the U.S. and Europe give redress to that European in that case. In the case of Canada, since we are not a country under the Judicial Redress Act, we cannot exercise these redress mechanisms. The only mechanism that is envisaged is the one that SECU, the national security committee, is adding to the pre-clearance agreement.

In substance, Europeans are subject to the same searches in the U. S. as Canadians, but by process, Europeans have a right of redress that we do not have.

Mr. Raj Saini: Can you be specific on the right of redress? What does that actually entail?

Mr. Daniel Therrien: I wish I couldn't. The U.S. has a relatively complex set of redress mechanisms, some internal to government, like ombudsmen for instance, and in some cases judicial redress. It's a complicated system.

Mr. Raj Saini: I have one final question. From my understanding, when a Canadian border officer searches a phone, that phone has to be disabled and that phone cannot connect to the Internet and it cannot connect to a cloud service. Is it true that the only thing searchable on that device is what's contained in that device?

Mr. Daniel Therrien: Under the policy of the CBSA, yes.

Mr. Raj Saini: On the American side, do they have that ability? Is the policy the same?

Mr. Daniel Therrien: No. The U.S law and policy are much more permissive for border officers. It is different. By policy, Canadian officers are restricted to look at what is on the device, but under the law, they could go much further.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thanks very much.

Mr. Kent, you mentioned you had a follow-up.

Hon. Peter Kent: Yes. It follows on from Mr. Saini's question.

You suggested earlier that if a traveller to the United States, or conversely to Canada, wanted to protect and manage data, they could park it on the cloud and then access it at their destination. Doesn't that suggest that already border security services, both Canadian and American, are somewhat behind the curve? There are those who might have criminal or other evil intent who would then be able to avoid the examination of a personal device and use the cloud to get around it. Besides the naive—

Mr. Daniel Therrien: If government officials on either side had suspicion about someone as a criminal, they could seek judicial authority for that information, even if it's in the cloud. The difference is that, to get that information that would be protected by a criminal, you would need a judicial authorization of some kind. At the border, it's much easier.

Hon. Peter Kent: Thank you.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Do you have a follow-up?

Mr. Nathan Cullen: I'm confused with the testimony to Mr. Saini and to Mr. Kent because you said that, essentially, the practice in Canada is not to allow our border agencies to take a device, search the device, and then use that device to search the person's cloud information. However, you said both law and practice in the U.S. would allow a U.S. border official to access the cloud through a device. In earlier testimony, you said perhaps if people were worried they could park information on the cloud and then re-access commercial or government information once landed in the U.S. Do you understand? I may have misheard you just as to how the advice given before seems to be contrary to what the reality might be.

Let's say I'm leaving for the U.S. I have highly sensitive government documents on my device, so I park them in the cloud. I go across the border, and they ask for not only my password for my phone, but they say they notice there's a cloud so they'd like the password for my cloud as well.

Mr. Daniel Therrien: In the United States, they could require that.

Mr. Nathan Cullen: Therefore, parking information in a cloud going into the U.S. is not actually going to do anything if I have sensitive documents that I would rather not have in the hands of U.S. border officials.

Mr. Daniel Therrien: That's a fair point.

Mr. Nathan Cullen: I just wanted to be clear. Again, I'm catching myself up to the technology.

We've noticed these executive orders that have come down from the current administration. In terms of the travelling public, what's the biggest change that's happened since the election of President Trump with respect to the issues that we're dealing with here today? Would there be one significant difference in the way that information is handled or sought versus under the previous administration, or is it more or less a continuance?

● (1705)

Mr. Daniel Therrien: We've not investigated the practices of the U.S. administration. The way I would answer is that the executive order on limiting the application of the U.S. Privacy Act gives a message to officials in the U.S. government that the data of foreign nationals is not to be protected. It's a general message. What the administration or what officials actually do with that message then depends on the intricacies of the operation.

Mr. Nathan Cullen: A signal was sent.

Mr. Daniel Therrien: It's a signal.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Mr. Zimmer, I believe, has a short question, and then I have a few questions.

Mr. Bob Zimmer: Again, thanks for coming. You talked about the deconstruction of data. I am familiar with databases and with them not being necessarily destroyed like expected. How do we have assurance from the federal government in the U.S. when it says that it's only going to retain specific information for a certain period of time?

How can we be reassured that if it says the information has been deleted that it actually has been? I hate to use that on record, but is it just a simple respect of the other country that it's going to do what it says it's going to do? How do we know if that data has been absolutely destroyed? What can we do if we're suspicious that it hasn't been? Is there any recourse for Canadians?

Mr. Daniel Therrien: It's mostly a matter of bilateral relations between the two states.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thank you.

With regard to Mr. Cullen's point, I would note that if I saved documents on my Google Drive and I don't have the Google Drive application on my phone, I can certainly cross the border. No one is going to search my Google Drive, and I can access it in the U.S. You'd have to delete it from your phone.

I just have a few questions. First, I take it that you are referring to CBSA bulletin PRG-2015-31. It refers to the Customs Act and to IRPA, and it sets out policy prescription for the CBSA officials with respect to the searches of electronic devices.

Ms. Patricia Kosseim (Senior General Counsel and Director General, Legal Services, Policy, Research and Technology Analysis Branch, Office of the Privacy Commissioner of Canada): Which number?

The Vice-Chair (Mr. Nathaniel Erskine-Smith): It's PRG-2015-31. This is the policy guidance that says that, under the Customs Act, paragraph 99(1)(a) is for customs purposes only, and mentions the multiplicity of indicators. With respect to IRPA, subsection 139(1) refers to reasonable grounds, that the purpose of the search should be confined to these issues, and that they must explain their reasoning. Certain protections are outlined.

Not for today, but if you could review that policy guidance from the CBSA, and if you have additional privacy protections that you would like to see the CBSA include in that policy guidance, it would be good to have that for our purposes at this committee.

I take your principal point here that the policy is generally wise, but it ought to be reflected in legislation. The first point is that we receive any additional guidance you have, and the second recommendation would be that it be reflected overall in legislation. That's on the Canadian side, as I understand it. We provide protections to Canadians and foreign nationals through the CBSA rules. None of those same protections apply if we're travelling to the United States.

We had the ACLU before us, and they said, as you've said, that the rules allow the government to search any travellers, regardless of citizenship status, and devices without a warrant, probable cause, or suspicion. You've mentioned the U.S. Judicial Redress Act. Are there any other measures or mechanisms that we should be asking our American counterparts to implement to protect Canadians' privacy, other than simply adding Canada to the designated list of countries under the JRA?

Mr. Daniel Therrien: I've asked three ministers of our government to essentially confirm that protection through administrative agreements—and there are a number of them—and whether they still protect Canadians despite the signal given by President Trump through his executive order. One part of the picture is to obtain confirmation by the U.S. government that these agreements continue to be in effect. That's certainly one way.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Have you received a reply in the affirmative from these ministers?

Mr. Daniel Therrien: I'm told that the Canadian government has obtained information from the U.S. government, and that I will be given a version of that information shortly.

● (1710)

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Will that same information be provided to this committee as well?

Mr. Daniel Therrien: Yes.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): If you could undertake to provide it to us, so that as soon as it's in your hands, it's in our hands, it would be appreciated.

Mr. Daniel Therrien: Yes.

There is also judicial recourse in the United States. Some American citizens are challenging the new U.S. policy, so that will find its way through the U.S. courts.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Do you have a counterpart in the United States that you work with on privacy issues? I ask because the ACLU said that in a 2015 privacy assessment from Homeland Security, there was the implication that downloading and mirroring of electronic devices was already happening at the border. I hate to tell you, Mr. Long, but all that information they looked at they might still be looking at, it seems, if they mirrored it.

Do you have an American counterpart you work with who looks into these issues on the American side?

Mr. Daniel Therrien: In the U.S., the system is somewhat different. There is no one counterpart. There are privacy experts in individual departments including Homeland Security who advise departments of privacy matters. They are not independent of the executive branch, as I am.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thanks very much.

You've given us a lot to think about in formulating questions for our American visit.

Does anyone have any other questions? If not, we'll adjourn until the next meeting.