HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Citizenship and Immigration

CIMM • NUMBER 052 • 1st SESSION • 41st PARLIAMENT

EVIDENCE

Wednesday, October 3, 2012

Chair

Mr. David Tilson

Standing Committee on Citizenship and Immigration

Wednesday, October 3, 2012

● (1535)

[*English*]

The Vice-Chair (Ms. Jinny Jogindera Sims (Newton—North Delta, NDP)): I'd like to call the meeting to order.

We are here for the ongoing study on ensuring that Canada's immigration system is secure.

Today we have two segments. During the first segment we'll have Benjamin Muller, professor of political science from King's University; followed by Dr. Mark Tyndall, professor and head, division of infectious diseases, at the University of Ottawa. You will each have 10 minutes to speak, and then we will have a series of questions.

I want to remind everybody that this is televised, just so everyone is aware.

Yes, Député Dykstra.

Mr. Rick Dykstra (St. Catharines, CPC): I have a couple of questions specifically to you, Chair, and it has to do with both of the individuals here, who, as I understand it, were your witnesses. These are witnesses you submitted to the clerk?

The Vice-Chair (Ms. Jinny Jogindera Sims): I believe.....

Mr. Rick Dykstra: Or it may have been Mr. Lamoureux. Both of them?

Mr. Kevin Lamoureux (Winnipeg North, Lib.): Yes, I believe they both are.

Mr. Rick Dykstra: Okay. Then the set-up is fine, because my questions are about process and how we're going to handle it this afternoon.

I certainly, obviously, want to thank witnesses who come to committee to present on behalf of their perspective on the issues we are dealing with.

I do have a question for Mr. Lamoureux, and that is that while Dr. Tyndall obviously has a great deal of background and research and understanding of issues pertaining to the health and welfare of those in our communities, I'm not sure—and I'd like to make sure and get your specific understanding on this—how his presentation is going to relate to the study of the security of our borders here in Canada.

The Vice-Chair (Ms. Jinny Jogindera Sims): Député Lamoureux.

Mr. Kevin Lamoureux: Thank you, Madam Chair.

I do find it a little bit surprising. Last Monday we were sitting here and we had a presenter. I believe it was a possible Conservative presenter who came forward and made his presentation based on multiculturalism. It was, I thought, fairly well received in terms of the members.

I would suggest to you that this particular witness you're referring to has a great deal of background knowledge. There are many refugees who come to Canada who might have issues surrounding health. I think it is appropriate. I would suggest we just continue on and listen to the presentations, and then go forward from there.

Mr. Rick Dykstra: Through you, Chair, I want to be fair to Dr. Tyndall. I don't have an issue with him presenting here today, but as you know, we did lay out as a subcommittee, which was later verified and agreed to by the committee, that we would be specific around the security issues relating to immigration. If you recall, this was one of the suggestions you made to have this study based on your readings of the Auditor General's report.

So if Dr. Tyndall is here today to speak to the issues of security as they relate to refugees and the perspective he has on that issue, I obviously have no problem with that whatsoever.

I just want to make sure that in fact it does relate to the security of those who are in this country and those who want to come to this country.

The Vice-Chair (Ms. Jinny Jogindera Sims): As chair, I want to say that areas of study that are included—just so we are all aware, because I know it has been awhile since we reviewed those—are biometrics, war criminals, security clearance checks, border security, visas, detention, and removal.

Mr. Rick Dykstra: If his presentation is pertaining to those issues, then I would like to hear what both Mr. Muller and Dr. Tyndall have to say this afternoon.

The Vice-Chair (Ms. Jinny Jogindera Sims): Back to Député Lamoureux.

Mr. Kevin Lamoureux: Madam Chair, I do appreciate the comments from the minister, and I do appreciate your comments as chair, but I think it's important to recognize that all political parties have the opportunity to invite guests.

You cannot tell me that the health and well-being of refugees is not relevant to this particular committee. Many refugees who come to our country are in need of health care services.

I don't want to, in any way, tell a witness what he can or cannot present. I'm sure he would have been made aware of what the committee is dealing with. I'm not going to censure his comments. I think we should just continue. It's a 10-minute presentation. When we had a witness here on Monday who only talked about multiculturalism, I didn't say, “On a point of order, let's be relevant”, and then dictate exactly what the chair just finished dictating. In fact, if we forced every presenter to adhere to what the chair just dictated, I suspect there would have been numerous points of order.

I don't think Mr. Tyndall should be singled out in any fashion whatsoever. He should be allowed to make his presentation. If you don't believe it's relevant and important to ask questions, I'll be more than happy to take the Conservatives' questions. We have two witnesses here. You don't even have to ask your questions of that particular witness.

I would suggest that it is in order and that we continue.

The Vice-Chair (Ms. Jinny Jogindera Sims): As chair, I was trying to show that there is an overarching—it's not just a very narrow definition of who appears as witnesses. At no time was I trying to narrow the field. From the chair's perspective, I do not see an issue with the witness, because he is going to be talking about one aspect of security.

Mr. Rick Dykstra: My intentions are not to do anything of the sort that Mr. Lamoureux is suggesting. I'm merely pointing out that we need to be fair to witnesses who come here. When they're making a presentation, if they aren't aware of or understand how it relates to the overarching security issue we're studying at committee, it puts them in an awkward position. It also puts me in an awkward position, as parliamentary secretary and lead on this side, to continually interrupt, or to question whether the discussion we're having is relevant to the study we're working through.

Rather than just be quiet and go through that process as he's presenting or as someone's asking questions, I thought it would be more polite to lay it out before the actual presentation started, so he would be aware, and also that I could, in all fairness, relate my concern to you. Obviously, you don't think it's a problem, so I'm going to assume it won't be.

● (1540)

The Vice-Chair (Ms. Jinny Jogindera Sims): Okay.

I've got a speakers' list and I want to stop this two-way dialogue, important as it is. You can maybe have that on your own later or get in line.

I have two other speakers, and I'm going to Député Menegakis first.

Mr. Costas Menegakis (Richmond Hill, CPC): Thank you, Madam Chair.

I would add my voice to what Mr. Dykstra said. I believe we need to stick with the terms of reference as they relate to the specific subject we are studying, which is security. If the witnesses, no matter who they are, were kind enough to appear before us and are testifying in accordance with the terms of reference in the invitation —I think that's what Mr. Dykstra was trying to bring up—we certainly have no problem.

The Vice-Chair (Ms. Jinny Jogindera Sims): Thank you.

Député Groguhé, go ahead.

[*Translation*]

Mrs. Sadia Groguhé (Saint-Lambert, NDP): Thank you, Madam Chair.

I have a point of order. It's important for us to be able to begin asking the witnesses questions. That being said, we all receive the list of witnesses, as many as we are. I think that, in good conscience, we invite our witnesses based on what we have to study. So far, I don't think I have noted any discrepancies between the testimonies of our guests and the study we are carrying out in committee.

This is just a point of order to accelerate the process and begin asking our witnesses questions. Thank you.

[*English*]

The Vice-Chair (Ms. Jinny Jogindera Sims): Député Lamoureux, go ahead.

Mr. Kevin Lamoureux: Thank you, Madam Chair.

I want to emphasize a couple of points. When we ask witnesses to come before the committee...it's important to recognize that you have 12 members of Parliament sitting in a very formal room. That, itself, can be somewhat intimidating to some witnesses. I'm not suggesting that Mr. Tyndall or other witnesses are intimidated per se by it, but it's something we should at least be aware of.

I don't believe that it is in fact appropriate for us to start every meeting dictating what we expect witnesses to be providing comment on.

If there's a government policy that has been made that in essence takes away health care services, for example, from refugees, does that have any sort of a risk factor? I would suggest to you that it could be a risk factor.

I don't want to tell a presenter what he or she can or cannot present. We're affording the people the opportunity to present before this committee on what they believe is important to them in relation to immigration and citizenship. In this particular case we're studying, as has been pointed out, we're hoping for a detailed report to be able to provide recommendations to the minister.

At the end of the day, if we believe there is a need to have a recommendation that says that reinstating health care services or anything of that nature will ultimately be better and improve the security of Canada, then we need to talk about it. If you have people who are denied the opportunity to be able to get some sort of medical treatment, for example, and they end up falling on the other side of the law as a direct result of that, I think that is something that is worthy of being able to talk about.

I'll leave it at that. I would hope—

The Vice-Chair (Ms. Jinny Jogindera Sims): I'm going to take a point of order. I just want to say that I think I've heard a fair bit of debate. I'm going to take the point of order, and then I'm going to make a ruling.

A point of order.

Ms. Roxanne James (Scarborough Centre, CPC): My point of order is that I think we really need to go in camera on this. My colleague across the way, Mr. Lamoureux, is talking about policies that we're not discussing in this particular session of our committee on security. I think if he needs to air that, it does not need to be done in front of the witnesses, who are here to speak to this committee.

So I'm going to put a motion forward that we go in camera to allow Mr. Lamoureux to continue talking about the other issues he has.

Thank you.

● (1545)

The Vice-Chair (Ms. Jinny Jogindera Sims): I'm trying to seek some guidance, because in the world I've lived in, I didn't know a point of order could lead to a motion to go in camera.

Mr. Costas Menegakis: It's a dilatory motion.

Mr. Kevin Lamoureux: [*Inaudible—Editor*]...she would get the floor had she not said a point of order.

On the same point of order, Madam Chair, just to facilitate what Ms. James is trying to do—

The Vice-Chair (Ms. Jinny Jogindera Sims): Mr. Lamoureux, I've got to first.... I'm trying to think through the rules of order here.

Mr. Kevin Lamoureux: I'm just trying to help out on the same point of order, if I can provide comment on it. I believe if you check with the clerk, I can do that.

The Vice-Chair (Ms. Jinny Jogindera Sims): It's non-debatable, so no comments.

Mr. Kevin Lamoureux: A point of order is debatable. I believe the floor was recognized as a point of order, so I should be able to address the point of order.

The Vice-Chair (Ms. Jinny Jogindera Sims): She moved a point of order, but then she actually moved a motion, and we're now dealing with the motion.

Mr. Kevin Lamoureux: A person does not move a point of order. A person stands on a point of order, and after the point of order is dealt with, then the person can move a motion.

All I was going to suggest—

The Vice-Chair (Ms. Jinny Jogindera Sims): Just make your comment.

Mr. Kevin Lamoureux: All I'm going to suggest is that I will conclude my comments, and maybe you can make a ruling on the point of order not being a point of order, and then Ms. James can move her motion.

The Vice-Chair (Ms. Jinny Jogindera Sims): I'm going to go back to Député James.

Ms. Roxanne James: Thank you.

I actually wanted to go in camera, but at this point in time I would really like to hear from the witnesses, as opposed to from my colleague talking about a bunch of other things that may have come before committee before, or that may be dealt with elsewhere, and not in this particular session that we're studying.

The Vice-Chair (Ms. Jinny Jogindera Sims): Thank you very much.

Ms. Roxanne James: So I prefer that we just move ahead with this particular witness.

The Vice-Chair (Ms. Jinny Jogindera Sims): Okay. That's what we're going to do right now. We're going to move on with hearing from the witnesses.

You have 10 minutes each, and we will start off with Benjamin Muller.

Dr. Benjamin Muller (Professor of Political Science, King's University College at Western University, As an Individual): All right.

Thank you for having me. I appreciate it.

Throughout the world, biometric technologies are used in border security to varying degrees. A panoply of machine-readable travel documents are increasingly prevalent, particularly among so-called trusted or registered traveller programs, as well as in permanent resident, green card, and visa schemes.

Even in these cases, serious questions regarding the continued potential insecurity of breeder documents tend to be ignored, and the dangerous consequences of social sorting are deliberately avoided. Social sorting refers to the manner in which increasing amounts of digital information on individuals begin to create a so-called data double, which, although desirable to marketers and law enforcement, has shown to be less effective in predicting risk and more effective in predicting your next purchase on Amazon.

Still, some jurisdictions have taken biometrics to a much higher level, such as the development at the University of Arizona of AVATAR—the automated virtual agent for truth assessments in real time—which is effectively something the size of an ATM machine and replaces a border agent, using artificial intelligence and biometrics to carry out a typical initial inspection.

In all these cases, there are significant questions that remain unanswered and relatively unexplored about biometrics.

Using these technologies as well as various other forms of surveillance have significant problems in terms of public buy-in. Certainly part of the problem is the lack of public participation in the process and the adoption of these technologies. It is often unclear why particular biometric technologies are adopted: what makes a specific biometric technology apt for a particular problem?

Like many tools, they oversimplify complex political, social, and legal networks according to a new classification of biometrically enrolled subjects.

There is what Joseph Pugliese refers to as “infrastructural diffusion”, where certain norms of gender, ethnicity, and socio-economic status are bred into the technologies themselves. A prime example would be the failure of facial recognition biometrics on African Americans tested at Miami-Dade airport.

The development and application of biometric technologies tends not to focus simply on helping to resolve with greater certainty "who" you are, but, with the increasing interconnection with other pieces of personal digital data, determines "what" you are. Are we aware and comfortable with the way in which this transforms our manage of the border and the mobile subjects who intend to cross it?

Beyond deeply important ethical, political, and social issues, there are straightforward problems with biometric technologies that deserve consideration.

A recent study at the University of Notre Dame, published in *Nature* magazine, found that the so-called false-match rate increased 153% over three years.

A five-year study released in September by the National Research Council in Washington, D.C., labelled biometrics as "inherently fallible": they only provide probabilistic results and not yes and no answers.

We are in dire need of increased research on the biological underpinnings of human distinctiveness. How stable the actual physiological characteristics are that the technology is designed to measure remains in serious question.

The AVATAR program, which is now being tested along the Arizona-Mexico border, biometrically measures 15 of 500 possible cues, which is lower than the 5% threshold set by the developers themselves. Happily for them, politicians are more excited about the gadgets than reflecting on the science they themselves have laid out.

There are some important questions we need to ask. What precisely do we expect these technologies to solve? What are the specific problems we believe they will address? Is the government willing to invest in public and intellectual engagement to consider seriously the specific efficacy, efficiency, and inherent problems associated with the use of these technologies? The research demonstrates that the industry is not compelled to do so on its own.

In conclusion, first, the signing of the Beyond the Border agreement already puts into policy what Nick Vaughan-Williams has referred to as the border not being "where it is supposed to be". It is clear that this agreement will compel Canada to engage on a variety of bilateral fronts on the management and enforcement of mobility and circulation, but the extent to which this has occurred with little significant public consultation, and to what extent it requires the total adoption of these specific biometric technologies, may still be something that is salvageable.

Two, the increased reliance on biometric technologies together with other forms of digital surveillance move us away from a question of who the person is to what kind of person this is. This significantly alters how the border operates.

● (1550)

Three, the United States and Europe have multiple skilled and effective independent and non-governmental institutions devoted to evaluating border security—the practices, strategies, and technologies to be applied therein.

Canada has none.

The absence of this capacity will do little to enable policy innovation, effectively evaluate the efficacy and efficiency of strategies to secure the border and enhance mobility, or move us away from being little more than reactive to the foreign innovations of other policies.

Thank you.

The Vice-Chair (Ms. Jinny Jogindera Sims): Thank you very much.

We'll move straight over to you, Dr. Tyndall.

Dr. Mark Tyndall (Professor, University of Ottawa, and Head, Division of Infectious Diseases, Ottawa Hospital, As an Individual): Thank you.

First off, I'd like to thank the committee for the invitation. It's a new experience for me. Building up to my talk, that's another new experience. Thank you for that.

As a bit of background, I'm a physician at the Ottawa Hospital with expertise in public health and HIV. I completed my medical school and internal medicine specialty training at McMaster University, followed by a fellowship in infectious diseases at the University of Manitoba. I went to the Harvard School of Public Health and completed a doctoral degree in epidemiology, and through this training I spent about four years in Kenya doing HIV research.

I took a job at the University of British Columbia in 1999 and spent about 11 years looking at HIV prevention strategies among marginalized populations, including drug users and refugees.

I moved to the University of Ottawa in 2010 to become the head of infectious diseases, with the goal of expanding the public health mandate of the division.

The clinic I am in charge of at the Ottawa Hospital has a large refugee caseload. As would be expected at an infectious disease clinic, we deal with infections. The biggest threats to refugee health, at least on arrival to Canada, are infections, most notably HIV and tuberculosis. On April 25, when Minister Kenney announced the cutbacks to federal health funding, the clinic physicians were in shock.

Currently, every major health care organization across Canada has spoken out in opposition and rallies against these cuts. Although the government has remained steadfast in its public announcements around the cuts, there have been a number of changes and rollbacks that have just added to the confusion.

We are now anticipating a list of designated countries of origin that will further limit access to health care for some refugee claimants.

There are many reasons that these cuts to IFH are bad for refugees, bad for health care, and bad for Canada. However, today I will focus on public health and why limiting access to health care creates a real threat to our collective public health security.

Of all the issues being considered by this committee, public health and the spread of disease should be recognized as a very serious threat to our security. It has been stated over and over by the Minister of Immigration and his staff that infectious diseases that are considered a threat to public health and safety will continue to be covered under the new IFH plans.

However, for all their resilience and optimism, refugees are generally scared and uncertain about their immediate future when they arrive in Canada. For many refugees, western medicine is foreign and unproven. It is only in the hands of skilled health care workers over multiple visits that trust is built and medical recommendations can be followed.

There is much more to treating HIV than providing pills.

One of the biggest health failures in confronting the global HIV epidemic has been a failure to appreciate the importance of providing a comprehensive set of health care supports for people who are HIV positive. In the United States, a study presented at the world AIDS conference this summer showed that of the estimated one million people infected, only 75% knew they were HIV positive, only 50% were receiving HIV care, and only 28% were successfully taking their HIV medications.

This is exactly what happens when people are not engaged in consistent health care. For the IFH program to continue to pay for the cost of HIV medications but fail to support the very care that makes successful treatment possible undermines the whole program. With these cuts, we are at risk of losing the patients who are currently engaged in comprehensive care, and we are much less likely to engage new patients in HIV treatment. We currently have the tools and expertise to diagnose and treat communicable diseases and limit their spread. However, if the patients are driven away and disengaged from health care, there is no way to identify infections and provide the necessary care, treatment, and education.

Tuberculosis is another serious threat to public health security in Canada. Unlike HIV, which will usually be picked up through mandatory HIV testing prior to arrival in Canada, tuberculosis is often asymptomatic and very difficult to diagnose. In many developing countries, the actual infection is picked up during childhood and lies dormant. The only way to diagnose and treat tuberculosis is to have consistent clinical care and to provide diagnostic testing at the first signs of cough, fever, or other more subtle symptoms.

The continued provision of medications to treat tuberculosis through the IFH is a small part of the necessary tools for early detection and the prevention of spread to others. The cutbacks will have a dramatic impact on the ability of public health to protect Canadians from the spread of imported tuberculosis.

There are certainly other threats to public health beyond HIV and tuberculosis; however, these examples serve to illustrate the very real threat to public health and security resulting from cuts to IFH. It is imperative that refugees are offered comprehensive health care to successfully integrate into Canadian society.

● (1555)

IFH funding provides a critical safety net as refugee claimants await the decision about whether they can stay in Canada or not. For communicable diseases, even a few weeks can be critical, and if the process drags on for years—which has been the case for a number of patients in our clinic—then the threat of spreading infectious diseases to others, both inside and outside their immediate community, is very real.

It is very predictable that we will start to see people defaulting on their HIV treatment and presenting with advanced HIV, and we will see women giving birth to HIV-positive babies. In addition, we will see people presenting to emergency departments with advanced tuberculosis, and there will be cases of tuberculosis transmitted within Canada from refugees. These are not far-fetched scenarios. In fact, they were happening before any cutbacks to IFH.

I feel that the cuts to refugee health care are short-sighted and will directly erode the public health care system that we have in Canada. In my view, this has a direct impact upon Canadian security.

Thank you.

The Vice-Chair (Ms. Jinny Jogindera Sims): Thank you very much.

I'm going over to Député Menegakis.

Mr. Costas Menegakis: Thank you, Madam Chair, and thank you to our witnesses for appearing before us today.

I'm glad we're getting this under way. I have prepared a few questions that I'd like to ask today. We are studying security, and a whole bunch of things come with that. I'm wondering whether I can get your view on a few things.

In your opinion, will the electronic travel authorization—ETA, as it's known—and the entry-exit provisions in the perimeter agreement prevent foreign criminals from abusing our generous immigration system?

Mr. Muller.

● (1600)

Dr. Benjamin Muller: I'm not aware of any data that would demonstrate that.

Mr. Costas Menegakis: Are you familiar with the ETA at all?

Dr. Benjamin Muller: Yes. I'm also familiar with the extent to which, when it comes to border security, for example, unless you have catastrophic failure, you tend not to be aware of whether something is effective or not. So, for example, if someone crosses the border, comes into the country, leaves again, and actually doesn't do anything, we have no way of knowing whether in fact that individual was a risky individual. Just because they chose not to act, we're unaware and may falsely put it down as demonstrating effectiveness.

Mr. Costas Menegakis: If you're familiar with ETA, then you are aware that the ETA will allow the government to know every time a single person enters or exits between Canada and the U.S., even at land crossings.

Dr. Benjamin Muller: Yes, I'm aware of that. The other issue is—

Mr. Costas Menegakis: Would that information not be useful?

Dr. Benjamin Muller: Sure, in terms of profiling. The unfortunate thing is that up to this point, in most cases profiling does not appear to be terribly effective. It certainly hasn't effectively stopped people such as Richard Reid or the underwear bomber—these sorts of individual.

The other point I would make is that the recent study specifically on biometrics suggests that one of the problems is that over time the biometric can become highly unreliable. In terms of repeat movement over a time period, that's a problem.

Mr. Costas Menegakis: I'm going to get to that; it's actually my next question. Just before I get to it, I want to stick with the ETA for a moment.

Do you think it will help the government crack down on residency fraud—people wanting Canadian status without living here or paying into the system?

Dr. Benjamin Muller: Possibly. I think if anything this would be a potential area in which it might be effective.

Mr. Costas Menegakis: Okay.

The impetus behind biometrics, the reason we are considering implementing it, is that it has been identified by law enforcement agencies who have testified before us as a 21st-century identification tool. I'm referring specifically to the RCMP, the CBSA, CSIS. They feel that this type of information would be very useful in identifying someone, particularly in cases in which someone has five or six or seven names in their name, have been refused a number of times because they were deemed to be a risk to the country, and have come back with a different derivation, if you will, of their name.

Do you think this is an effective tool for preventing fraud and keeping security threats out of the country?

Dr. Benjamin Muller: It's not as effective as, shall we say, human intelligence. My research has not indicated that there's any reason we ought to simply be jumping on board the use of biometrics.

I'm well aware that law enforcement agencies tend to be reasonably happy with it, until you get to the sort of high point of it, which I would say is what the AVATAR program at the University of Arizona has come up with, because then it starts taking their jobs away. You clearly and obviously have labour issues at that point.

But in terms of gathering information, it's good to gather information. What you do with it, how interoperable those bits of information are.... I think there are obviously privacy questions as well as questions of reliability. For the most part, I feel that these biometric technologies are relatively under-studied. That's why we're only now getting some of the longer-term studies, which are what is useful.

At the moment, most of the research we get is from the manufacturers themselves, and I don't think I need to tell everyone that there could be problems with that.

Mr. Costas Menegakis: Certainly the manufacturers and the biometrics have been tested by law enforcement agencies before they recommend them, but let's talk from a practical perspective.

You speak about human intelligence as being an alternative. If someone shows up at our border today—right now, as we speak—and says, "I want to come into your country", there's an officer there who will be looking at and interviewing them as they are going through this process.

He doesn't know who you are; you could tell him anything. With a biometric, he can look you up in a computer, with your picture, possibly your iris scan, and your fingerprint, and he'll know exactly who you are.

Would that not be a useful tool for that intelligence officer?

It's not a question of coming in without having human interaction anyway. No one is saying that someone is going to walk to the border, walk into a booth, and the door will open and they'll get into Canada. There will be a person there who's going to be using that as a tool.

That's what the law enforcement people who presented before us testified: that it's an additional tool they could use to help them in the identification of an individual. The whole point of this is to ensure that we know the identities of individuals before they walk our streets, shop with our families, or are around our kids. We need to know who they are. That is the main thing they kept bringing up to us.

Do you not think that could be a useful tool for a CBSA agent at the airport or someone at the border to have in deciding whether they're going to allow someone into the country?

● (1605)

Dr. Benjamin Muller: If we assume that the technology can't be defrauded, I would agree with you. But there is increasing research that suggests one can basically mess with biometric readings. High-resolution photographs, for example, will get you past facial recognition technologies, in some cases.

Mr. Costas Menegakis: And fingerprint—?

Dr. Benjamin Muller: Fingerprinting is actually one of the easier ones. Of course, it happens to be a cheaper one as well, so it's more prevalent.

Mr. Costas Menegakis: Isn't it a little bit more secure than someone just making a judgment on what you're telling him?

Dr. Benjamin Muller: A judgment has been made when that biometric—

Mr. Costas Menegakis: No, I mean in addition to that.

The Vice-Chair (Mr. Kevin Lamoureux): You have ten seconds left.

Mr. Costas Menegakis: My seven minutes are up?

Dr. Benjamin Muller: To assume that those judgments are somehow not made with the use of biometrics.... They still are. There's a sort of misapplied faith, in a sense, to the technology.

Mr. Costas Menegakis: Thank you very much. My time is up.

The Vice-Chair (Mr. Kevin Lamoureux): Ms. Sims, you have seven minutes.

Ms. Jinny Jogindera Sims: Thank you very much.

I'm going to direct my first couple of questions towards Dr. Tyndall.

I want to thank both of you for coming to make the presentation. I appreciated the presentation you made about public health. There isn't a greater area of security, for me, than public health. It's one that has no boundaries. So thank you for your presentation.

Often, when we sit around and think about security, we only think it means what happens at the border and that it's about deportation. But we know that security works both ways, and that we must ensure the safety and security of newcomers, especially vulnerable refugees. And security of health is very critical.

You've had first-hand experience, Dr. Tyndall, with treating refugees at the hospital. I'm interested in how the cuts to the interim federal health program for refugees are impacting their security.

Last week, Doctors for Refugee Care released a report that said:

> Three months after dramatic cuts to federally funded refugee health care services took effect, the program that manages these services is marred by confusion, unnecessary costs, and compromised care.

The report goes on to detail dozens of cases and says that pregnant women and children are being particularly affected by the cuts.

In one particularly shocking example from the study:

> A young female refugee claimant is 18 weeks pregnant as a result of a sexual assault while being used as a sexual slave. She has no IFH coverage to address the pregnancy.

Can you share with the committee any cases you are aware of and how the cuts are affecting the refugees you see?

Dr. Mark Tyndall: Sure. Thank you very much.

The report that was submitted last week showed a number of cases. In Ottawa itself there are probably 50 people in the clinic with some IFH coverage. Many of the people we see are being treated for tuberculosis and HIV. As I mentioned, the treatment of these two infections is still protected, and people still get their pills.

Most of the people, then, have already had a relationship with us, and they continue to get their pills. What is problematic now, however, is other services that they need. They come to a clinic with hypertension, for instance, or some have diabetes. They're running into difficulties with getting these medications covered and they have no fallback.

So there are cases of people we're still following for their HIV who no longer get coverage for their other medications, which in some respects have everything to do with their HIV infection.

Picking out only the pills for their HIV is not enough.

The Vice-Chair (Mr. Kevin Lamoureux): Dr. Tyndall, I have a point of order from Ms. James.

Ms. Roxanne James: Thank you.

I believe this is a point of order.

We said at the beginning that we are studying border security. I listened very intently to Ms. Sims' questions and nowhere did I hear a question such as how can we prevent people from coming into the country who have communicable diseases, as opposed to just case studies or examples of someone who is already here and who may have been asked to leave.

I just want to redirect the committee back to our original focus of this study, which is on border security, and I would hope that future questions will be dealt with in that particular strain.

Thank you.

● (1610)

The Vice-Chair (Mr. Kevin Lamoureux): In regard to it being a point of order, Ms. James, the committee has demonstrated, and we could probably cite back to the last time we met in terms of the types of questions and answers that were being given.... I believe this is, in comparison, just as relevant. But I appreciate the sensitivity on the issue, so I'll say it's not a point of order.

I will let Dr. Tyndall continue and hopefully we can get through the process.

Dr. Mark Tyndall: I can also comment, as you were asking what happens to new patients coming, that doctors cannot be put in the position to be the border guards. People get to the clinic and seek medical attention long after all these safeguards have been put in place.

So part of our concern is that some of our tools are taken away from us through these cutbacks. People who come really need health care, and some of that health care can be very important to the community at large. They will not be able to access that any more.

As doctors, the program right now is in such disarray that we're only told to call Blue Cross and find out if this particular diagnostic procedure or drug could possibly be covered for a specific person. Obviously it takes hours to get that information back, and the person is there. Currently, as things change, it's a moving target, where most clinics now are in a very bad way when they see new patients come to them. I have no control over who comes to the clinic.

If they have a problem—in my case, an infectious disease problem—I feel, as a physician, it's my duty to provide them the best care that I can. Saying “I'll have to check to see if I can provide you with any care” is difficult.

Ms. Jinny Jogindera Sims: Thank you, Dr. Tyndall. I have a very short time and I do have another question for you. And thank you for focusing in on infectious diseases, which definitely has a lot to do with our overall security.

A particularly troubling aspect of these changes, the ones that have been made recently, is that potentially legitimate refugees from so-called safe countries, under the recently passed legislation, Bill C-31, will be cut off from even basic medical coverage. Eventually we will learn what these so-called safe countries are, but we don't know yet.

Can you talk about how the cuts affect these particular refugee claimants, especially when it comes to infectious diseases and overall security?

Dr. Mark Tyndall: My understanding is that some of that class will receive no health care whatsoever. From a public health point of view, I think that's a disaster. People do have infectious diseases that they need to be treated for to protect our public health system, and if they are denied any care at all, it's really a problem for our own security and our public health system.

Ms. Jinny Jogindera Sims: Do I have another minute?

The Vice-Chair (Mr. Kevin Lamoureux): You have a minute and eight seconds.

Ms. Jinny Jogindera Sims: Thank you very much.

Once again, I do want to thank you.

One of the things I've realized as we've looked at this is that we do have provinces like Manitoba where they have said that they will actually be covering, on an interim basis, some of the people who are not covered right now. But I believe my colleague will be following up on that in more detail during the next round.

Thank you.

[*Translation*]

The Vice-Chair (Ms. Jinny Jogindera Sims): Go ahead, Mr. Lamoureux.

[*English*]

The clock has started.

Mr. Kevin Lamoureux: Thank you, Madam Chair.

I do appreciate both presenters' comments.

I want to go to Dr. Tyndall in regard to individuals who come as refugees to our country. Do we have a sense, in terms of a percentage, or can you give us any indication as to how many would be coming as refugees who would have some sort of medical condition? Can you provide comment on that?

Dr. Mark Tyndall: Everybody who comes is entitled to a first examination, where a lot of things are screened. I would say that infectious diseases in this population are high. People have come from very bad situations. I don't have the numbers off the top of my head, but I would think that well over 50% of people who are screened need some kind of diagnostic procedure or medical intervention, including treatment, so quite a high proportion of people.

● (1615)

Mr. Kevin Lamoureux: One of the diseases you referred to is tuberculosis. I have a tough time saying that word. That is something that is not identified right away. It takes time to identify that disease. Is follow-up required?

Dr. Mark Tyndall: I think tuberculosis is the best example where these cutbacks will have the most impact.

If we're telling people their access to health care, treatment, and diagnostics is limited, they won't go to a doctor. Most people who come from developing countries were exposed to TB in early life. A disease comes up at no predictable time. A lot of people will present to their family doctor and say they haven't been feeling well for a few days, that they have a cough or a fever. That needs to trigger an X-ray and further diagnostic tests. Unless there's ongoing follow-up, we're bound to miss, or certainly have a delay in, our ability to recognize tuberculosis. That's already a big problem in Canada. People, especially first nations people, have very high rates of TB. We do our best to screen people, but TB is one thing that can really get out of hand if we don't have ongoing comprehensive care for people coming from endemic countries.

Mr. Kevin Lamoureux: The spread of disease is a security issue when individuals are coming into Canada. Quite often it takes a while to determine whether or not someone is infected. Your suggestion is that we need to continue to provide those medical services because it's in the public's best interest to do so.

Dr. Mark Tyndall: It's definitely in the public's best interest.

From many aspects, even with many chronic diseases, we have great evidence to show that preemptively dealing with these saves us a lot of money and problems in the long term. Denying people basic medications for diabetes, hypertension, and asthma from a public health point of view makes no sense. If we're talking about infectious diseases, waiting until people present to the emergency room with their active tuberculosis means there's a very good chance they have exposed many other people. This is not something where they may have just infected their family members. This is the kind of infection that can be transmitted in shopping malls, bowling alleys, wherever people may go. It becomes very difficult to find people before they have already transmitted to others.

Mr. Kevin Lamoureux: Thank you.

The Vice-Chair (Ms. Jinny Jogindera Sims): You still have a minute and a half.

Mr. Kevin Lamoureux: Mr. Muller, I want to follow up in terms of biometrics. It is something we are hearing a lot about from the government and other stakeholders, that this seems to be the answer to many of the issues related to security. Live biometrics include fingerprints and live pictures, from what I understand.

To what degree do you think Canadians should take comfort in biometrics as providing security?

Dr. Benjamin Muller: I don't think any technology in and of itself provides security. It's the way in which it's used.

In the case of biometrics, I have studied the use of it in border security for about a decade now. There simply is not sufficient data to demonstrate that when in fact it is used it provides increased security. One of the problems is there is not a clear “problem” that it is being introduced to deal with. For example, with the U.S. visit system, there is no clear evidence that the United States is necessarily more secure. It simply is not there. The flow of migration, particularly at its southern border, continues with the use of AVATAR. Those things continue. Yes, you can create more profiling, but the extent to which that is in fact useful is not clear. There is no evidence.

Mr. Kevin Lamoureux: Do you find there are conventions—

The Vice-Chair (Ms. Jinny Jogindera Sims): Thank you very much. You are done.

Député Opitz.

Mr. Ted Opitz (Etobicoke Centre, CPC): I'm going to give Mr. Dykstra a moment or two.

Mr. Rick Dykstra: I just want to clarify a question you asked, Ms. Sims, which was actually incorrect in terms of your assumption that refugees who come, whether it's one of these infrequent arrivals, would not receive interim federal health care. They would in fact receive interim federal health care from the federal government. You asked Dr. Tyndall to respond to a question, which he rightly did. The basis upon which you made your assumption is actually incorrect.

I think the record needs to be clear that interim federal health care is available to those who apply for refugee status here in Canada, especially when we have an arrival, as we did, with the *Sun Sea* and *Ocean Lady*. That still falls into place. The level of health care they receive is different from the level it was prior to the changes that we've made, but indeed they still receive interim federal health care.

● (1620)

The Vice-Chair (Ms. Jinny Jogindera Sims): My understanding is that irregular arrivals arriving from a safe country do not receive any interim federal health care benefits until they have been accepted as a refugee.

Mr. Rick Dykstra: Well, I'm not sure we've ever had an irregular arrival from a safe country, but if that were the case, in fact, they would receive it until they've had their determination.

Mr. Kevin Lamoureux: If you want clarification, I can provide some, if you like, on that issue.

Mr. Ted Opitz: That's okay, because it's chewing up the rest of my time.

Mr. Rick Dykstra: No, in fact, it shouldn't chew all of it up. My statement might have, but not the response.

The Vice-Chair (Ms. Jinny Jogindera Sims): In going over to you. I'll let you deal with it.

Mr. Ted Opitz: Thank you.

Mr. Muller, you're referring to the research you do. Is it academic research, or have you done field research on biometrics?

Dr. Benjamin Muller: I have gone to Arizona to witness the use of the AVATAR program. Nogales, Arizona, is a city that's actually cut in half by the U.S.-Mexico border. I've also spoken to both American and Canadian border agents, basically, about the use of biometric technologies.

I'm not a scientist; I'm a social scientist.

Mr. Ted Opitz: But that machine you referenced is in trial stages right now. It's not deployed.

Dr. Benjamin Muller: It has been in trial stages. Well, it is now being used in that instance. It has been trialled in Europe for two years already.

Mr. Ted Opitz: What about a roll-out? Is it rolled out or is it still on trial?

Dr. Benjamin Muller: It's being used in the SENTRI system right now, so the interview you do for SENTRI—the U.S-Mexico equivalent of the NEXUS program—is currently being done in that location by the machine.

Mr. Ted Opitz: Okay.

Do you have a NEXUS card, by the way?

Dr. Benjamin Muller: I do.

Mr. Ted Opitz: And how do you find it's working?

Dr. Benjamin Muller: I actually got it as part of the research I did in 2008 at the Border Policy Research Institute in Washington State.

Mr. Ted Opitz: I have one as well, and I find it's worked quite well. It's biometric: they take the eye scan, they take your fingerprints, they take a photograph. So they do understand who it is that is coming and going through that particular system. I would suggest to you, sir, that this is relatively reliable overall, and it does provide a certain convenience of travel for travellers and others.

How long do I have, Madam Chair?

The Vice-Chair (Ms. Jinny Jogindera Sims): You have another three minutes.

Mr. Ted Opitz: Okay, good.

You also referred to human intelligence as an option to biometrics, or an augment. How is human intelligence gathered in this case, or HUMINT, as it's often called?

Dr. Benjamin Muller: I'd say two things. First of all, on your NEXUS point, yes, it's convenient. It also doesn't prevent fraud. In fact, some suggestion is that it can in fact enhance it because the breeder documents required to get to NEXUS are no more secure. The document you then receive on the basis of potentially fraudulent documents is then assumed to be more secure, and we then operate according to that assumption.

Mr. Ted Opitz: Yes, but you're not just giving this based on that alone. You're still getting an interview from both sets, Canadian and U.S. To your point, there is a human being also making a determination. But let's leave that alone.

Let's go to human intelligence. How is human intelligence gathered, in your view, for use in immigration and border crossings?

Dr. Benjamin Muller: I think for me the issue is that even in the case of NEXUS, once you have the card, your human interaction decreases.

Mr. Ted Opitz: That's not gathering human intelligence. How do you gather human intelligence?

Dr. Benjamin Muller: It's by talking to people. I think assuming that a technology is going to take that place, and then making assumptions that these individuals who now carry a card or have participated in a program are more secure on the basis of the fact that they've put their fingers and retinas up for digitization—there's simply not data to support that this in fact enhances security.

● (1625)

Mr. Ted Opitz: Yes, but that's not entirely human intelligence. Human intelligence is gathered. For example, if you're looking at criminal groups trying to infiltrate a particular country, human intelligence is gathered through the discussion of groups in those countries. You can get that information through refugees. You can get that information through travellers and others. And it's a compilation of intelligence that's built up. Talking to an individual across a kiosk is not human intelligence, sir.

Dr. Benjamin Muller: Right. But these programs that are being suggested are based on a variety of interoperable biometric data, and then creating a profile of an individual, based on their movement according to your entry and exit and so on. So there is an extent to which that is going to take the place of what you just suggested.

Mr. Ted Opitz: I think we can all agree that nothing is 100% infallible, for sure, but I think biometrics will allow an ability for our country and others, with shared data use and shared intelligence, HUMINT and otherwise, to protect our country. I think these biometrics...even if it's a 90% solution, or a 97% solution, it is valid in making sure, or helping to make sure, that people who have infiltrated our country in the past and have been deported for criminal acts don't get back in.

Would you agree that this is a valuable tool in terms of biometrics and being able to protect our security and our families, as Mr. Menegakis referred to earlier?

Dr. Benjamin Muller: I'd agree that it's potentially a valuable tool, but statistics like 97% and so on...that is not what data demonstrates.

Mr. Ted Opitz: The thing is, you didn't provide any data today. You're saying studies show this and studies show that.

Dr. Benjamin Muller: I listed two recent studies, one by the University of Notre Dame and the other by the National Science Council in Washington, D.C., both showing issues, false positives in the neighbourhood of 150%.

The Vice-Chair (Ms. Jinny Jogindera Sims): Thank you very much.

In order to let our guests know, I don't mean to be rude, but we do have very specific time allocations for each MP, and we want to make sure that every MP gets their turn.

So that the committee is aware, as a result of us starting a little bit late with this, the clerk and I did split the time difference, so that both segments today would have equal timing.

I would now like to go over to Sadia.

[*Translation*]

Mrs. Sadia Groguhé: Thank you, Madam Chair. I want to thank our two witnesses for joining us today. My question is for Mr. Tyndall.

You have presented the IFHP as a necessary safety net when it comes to public health and said that limiting health care would be a disaster. We fully agree with that opinion, especially since preventive health care is both more humane and more economical than curative health care.

The International Covenant on Economic, Social and Cultural Rights recognizes that everyone is entitled to the best physical and mental health status they can achieve and that states have a non-discriminatory obligation in the fulfillment of that right.

What do you think about those provisions? Do you think they can be ignored within the framework of public health?

[*English*]

Dr. Mark Tyndall: Thanks for the question.

Obviously, I don't. As this issue goes further and further, we've been careful not to push it to exclude any possibility that we can at least get the value back in what we had. There is a whole movement that everybody should be treated exactly the same, that health is a basic human right and that this should be offered to everybody.

At this point in time, I think the IFH, as it was, doesn't go to that extent. I think strategically, even if that's ultimately what I would support, feeling very strongly that health is a human right, at this point the cutbacks have taken us so far away from that that we're trying to battle to at least get some basic coverage back.

I think it reflects very badly on Canada if we deny health care to people. I'm amazed at stories I read in the paper about animals being helped out. We would not deny health coverage to any Canadian, so —

The Vice-Chair (Ms. Jinny Jogindera Sims): Hold on one second. I'm sorry.

Mr. Dykstra.

Mr. Rick Dykstra: I don't have any problem with anyone disagreeing at a certain point. That's the way democracy works. But if Sadia's questions are going to relate to health care, I feel that you, as the chair, could make the determination, while the question is being asked, that if it's relevant to security, no problem, but if it's relevant to what the health committee should be studying, then I would submit that that's the time to interject and say make sure it relates to the committee work that we're studying and not something that may very well be a health care issue that could be debated at the health committee. But certainly not from a security perspective did this have anything to do with the safety and security of our borders.

● (1630)

The Vice-Chair (Ms. Jinny Jogindera Sims): Okay.

Let's go over to Député Lamoureux.

Mr. Kevin Lamoureux: It's to the same point.

Madam Chair, if the member was actually doing this through a point of order, I think what we have to do—because I do believe the presenter was very relevant to the actual question—

Mr. Rick Dykstra: I'm not asking your opinion; I'm asking the chair's.

Mr. Kevin Lamoureux: And I'm advising the chair—

Mr. Rick Dykstra: You and I have had this discussion already. I know what your opinion is.

Mr. Kevin Lamoureux: All right. My advice—

Mr. Rick Dykstra: You brought a motion forward that was defeated, actually.

The Vice-Chair (Ms. Jinny Jogindera Sims): The chair is going to call for order from all sides, and if people could go through the chair....

I was asked by Député Dykstra to make a determination, and I am going to do that. In the meantime, Député Lamoureux had a point of order, or whatever, so he has a right to make his...and then I believe Sadia has a comment. I will make a ruling after that.

Mr. Kevin Lamoureux: Madam Chair, it's a very simple issue. I do believe the presenter was relevant to the question, and if there is going to be an interruption, it should be after the question itself is asked.

If the member had a difficult time with the question being out of order, that's one thing, but he was relevant to the question itself.

The Vice-Chair (Ms. Jinny Jogindera Sims): Thank you, Député Lamoureux.

Député Sadia, on a point of order.

[*Translation*]

Mrs. Sadia Groguhé: Yes, Madam Chair.

I just wanted to point out that it's important for witnesses to be able to finish answering a question. I don't think that interrupting them all the time is the role of the members in this committee.

I wanted to point that out, Madam Chair. I think it's important to remind all the committee members of that.

[*English*]

The Vice-Chair (Ms. Jinny Jogindera Sims): Thank you very much.

Député Groguhé has the time to ask her questions, and I'll go over to Dr. Tyndall to continue answering them.

Everybody is aware that the questions all relate to security.

Thank you.

Dr. Mark Tyndall: I think I was pretty much finished.

The Vice-Chair (Ms. Jinny Jogindera Sims): Thank you.

Back to you, Sadia. Do you have another—

[*Translation*]

Mrs. Sadia Groguhé: Yes, I have another question.

[*English*]

The Vice-Chair (Ms. Jinny Jogindera Sims): You have lots of time.

[*Translation*]

Mrs. Sadia Groguhé: My second question is for Mr. Muller.

You talked about the overall limitations of biometrics and technology in security. In one of your articles, you talk about the fetishization of biometrics and conclude with three recommendations: carry out an in-depth review of the risk management approach; do not treat technological measures as a cure-all; and consult the affected communities and stakeholders more about border management.

Are you recommending that to the committee again? Could you elaborate a little on that?

[*English*]

Dr. Benjamin Muller: Thank you.

Yes, I would stand behind those recommendations.

The application of risk management and the way that has occurred is very much connected to the deployment of these technologies, so I think examining that relationship is very important.

As these sorts of experiences tend to endlessly confirm for me, there is a quick reaction to looking at numbers that suggest that somehow biometrics are good, full stop. There are very rarely specifics ever given, in terms of a precise issue it will deal with at the border that is currently not dealt with sufficiently. I think that's a significant issue.

The other issue is that the public in general, and particularly those who inhabit border communities, often tend not to be terribly favourable in terms of wanting the use of these technologies.

In the NEXUS case, there's a reasonable enrollment because of lifestyle. But studies have shown—and there have been quite significant studies done on the Washington-B.C. border about this—that many people have chosen not to enrol in the NEXUS program, to stay in the lineups, simply for the fact that they have questions about the use of this technology and the way it can create this sort of "data double" issue, where a variety of pieces of data are linked together to create a persona that may or may not be a reasonable approximation of you.

Are we happy to make judgments on that basis, not to mention that increasingly data is demonstrating that these are not infallible technologies, by any stretch of the imagination?

When the designers of AVATAR themselves say their technology does not meet their own threshold, I think that's rather significant. But in that case, it's not significant to those willing to buy in to it.

● (1635)

The Vice-Chair (Ms. Jinny Jogindera Sims): You have a minute and a half.

[*Translation*]

Mrs. Sadia Groguhé: We had a witness—

[*English*]

The Vice-Chair (Ms. Jinny Jogindera Sims): Pardon me, my apologies. It was five minutes and your time is up.

[*Translation*]

Mrs. Sadia Groguhé: Already?

[*English*]

The Vice-Chair (Ms. Jinny Jogindera Sims): I just wanted you to get your hopes up there for a second. I thought you had seven minutes.

Earlier on I heard a response about a study you had to demonstrate the responses you were giving to Député Opitz. Is it possible to get it to the committee so that we have that available for us to read?

Dr. Benjamin Muller: Yes. It's not a study I completed, but I can certainly submit that information to the committee.

The Vice-Chair (Ms. Jinny Jogindera Sims): That would be great. Thank you very much.

I'm going to suggest that we take a three-minute break, and then we will resume with the second part.

I want to thank you both, Dr. Tyndall and Benjamin Muller, for the presentations you made. Let me assure you that we're not always this entertaining.

Voices: Oh, oh!

The Vice-Chair (Ms. Jinny Jogindera Sims): Thank you.

● (1635)

(Pause)

● (1640)

The Vice-Chair (Ms. Jinny Jogindera Sims): I'd like to call the meeting to order, please.

We have two speakers for this section. I don't know whether both of you are speaking or only one of you.

Mr. George Platsis (Program Director, Centre of Excellence in Security, Resilience, and Intelligence, Schulich Executive Education Centre, As an Individual): I'm going to tee it up, and then my partner is going to take over.

The Vice-Chair (Ms. Jinny Jogindera Sims): Okay.

We have George Platsis and Donald Loren. Welcome. You will each have 10 minutes to speak.

Mr. George Platsis: We had arranged for 10 minutes combined.

The Vice-Chair (Ms. Jinny Jogindera Sims): Ten minutes combined is even better. You will have 10 minutes to speak, and then we will have a round of questions.

Just so you know, the meeting is televised. If you need to use the audio devices, they are right there in the table, and you may need them at one time or another. But you may be perfectly bilingual, in which case you don't need them.

Without further ado, we'll go over to you, George.

Mr. George Platsis: Thank you.

We thank the vice-chair and the members of the committee for inviting us to appear before you once again. My name is George Platsis. I am a program director with the Centre of Excellence in Security, Resilience, and Intelligence at the Schulich School of Business at York University in Toronto.

With me today is one of our centre's senior distinguished faculty members, retired Rear Admiral Don Loren of the U.S. Navy.

Please note that our comments are our own today and do not reflect the views of any of the organizations we may be associated with.

The realities of the 21st century have shown us that technology has given access and ability to a larger number of actors, including small groups and individuals, all with differing intents and interests. The net result, even for a single actor, can have an asymmetric effect upon society.

Discussions focused on Canada's immigration policy, which are vast and broad, will define our ever-evolving Canadian identity, economic success, and security landscape. But for the purposes of this conversation and this session we will focus on a very narrow range of issues specifically related to intelligence-gathering capabilities and information handling, both domestically between departments and internationally with our partners and our allies.

Technology should be used as a tool, not as a crutch, and the foundation for any technology to protect our borders is intelligence. From information gathering to analysis to intelligence that is actionable, we need to ensure that the information we collect and analyze is kept confidential, maintains its integrity, and is made available only to those who have a legitimate use for it.

This issue is daunting in an inter-agency and international context, especially as organizations use differing levels of internal security protocols. Consider that on the issue of admissibility, upwards of 10 or more Canadian departments and various statutes could apply. Depending on the case, you have IRPA, the Security Offences Act, the National Defence Act, the CSIS Act, and the Aeronautics Act, just to name a few that could apply. In the example I just gave, CIC, the RCMP, CSIS, CSEC, and CATSA would all have some jurisdictional responsibility. And we have yet to consider our international possibilities.

In addition, the creation of Shared Services Canada has tasked it with streamlining more than 100 e-mail systems, 300 data centres, and more than 3,000 overlapping and uncoordinated electronic networks.

While this decision should reduce inefficiencies, there are other inherent risks associated with a fully integrated system. As we become more reliant on these systems to store personal information and make critical decisions, we also have a responsibility to harden these same systems, both from a technological perspective but also from a human-use perspective.

These same principles must also apply to more sensitive areas that fall outside the mandate and domain of Shared Services Canada; these relate to our national security. There's a very simple concept that we must never forget: you are only as strong as your weakest link.

Going forward, we must be able to assure the information we acquire and use. In an information-sharing context, this requires both human and technological safeguards. Furthermore, our own Canadian ability to gather, validate, and protect information from our uniquely Canadian vantage point benefits Canadian interests and intents as we go forward, so that we can make our own assessments that meet our own needs.

Ultimately, it should be sound information that acts as the basis for admission into Canada. We must be cognizant that, given that our systems and networks are interconnected, an information breach in one department may have an effect in many others, including upon the decision-making process for admissibility.

It is at this point that I would like to invite a very great friend of Canada, Admiral Don Loren, to share and give you the benefit of his experiences in these matters from an American and international perspective.

Thank you.

● (1645)

Rear-Admiral (Retired) Donald Loren (Senior Distinguished Faculty, Centre of Excellence in Security, Resilience, and Intelligence, Schulich Executive Education Centre, As an Individual): Thank you, George.

Madam Vice-Chair, members of the committee, thank you for having me here again. I'm a great friend of Canada, and it is at my colleague's request that I appear before you.

Please note that all the comments made today are my own and are not reflective of any organizations I may be affiliated with.

As noted in my previous testimony before this committee, I'm not here to address any laws in specific terms, as it is not my place as an American to do so. What I can offer is my perspective as the former deputy director for operations support at our National Counter-terrorism Center. As the former Deputy Assistant Secretary of Defense for Homeland Security Integration, I can offer my specific observations on issues of intelligence gathering, information sharing, particularly within the inter-agency and international context. I can also give you a view to assist you to define your own unique Canadian interests as they may relate to immigration policies.

The degree to which we can be proactive is the degree to which we both shall succeed or fail as we face the challenges that lie ahead for both our nations. Within that context, the challenges that both Canada and the United States face with respect to border security and immigration can only be resolved through both nations working together, as we have done in the air and missile defence of North America through NORAD.

The key to working together is to ensure that not only are the policies and programs implemented in both nations aligned, but that each nation is comfortable with the measures that are in place to address our customs and immigration challenges.

I can state that in my professional experience, addressing these challenges is not only about ensuring that the necessary equipment and resources are in place, but equally, if not more importantly, it's about ensuring that the intelligence and law enforcement information upon which decisions are based is sound.

For example, biometrics are often presented as a potential solution to solve many of the immigration issues we both experience, but it would be naïve to believe that implementing expensive technical solutions without the necessary intelligence to inform the technology is the sole answer.

Canada's membership in the Five Eyes provides access to significant amounts of information that can be used to better assess the potential risks posed by individuals attempting to enter the country. This information must be readily available to the appropriate decision-makers and shared across agencies, something that both of our nations can do better. Even if the information were made available and utilized properly, there are secondary and tertiary concerns that must be addressed before courses of action are undertaken.

For example, the security and assurance of the information must of course be protected. This means it is paramount that the infrastructure and architecture of the security and intelligence apparatuses used create a level of confidence amongst Canadian allies in order to have a more open flow of information, as this information will ultimately help ensure that only legitimate persons enter Canadian territory.

The strong relationship between Canada and the United States must always consider political dynamics that face our respective countries, as these same political dynamics could have significant impact on moving border and inter-agency initiatives forward. A mutual respect and understanding of the political winds of both countries should be considered when any courses of action are taken, thus ensuring that there are no misconceptions or misunderstandings.

The United States works hard to ensure that its border, immigration, and security policies are corrected, as does Canada work hard on these very same issues. Our nations have built our relationship on trust and mutual cooperation, and that should continue to be the case. As we work to constantly improve that sense of trust, that spirit of cooperation, and the practice of sharing information between nations, we must each work on similar relationships between our own departments, ministries, organizations, states, and provinces.

We must constantly strive to eliminate the cultural and procedural barriers that exist within our own nations and across domestic departments. We must consider ways to collect vital information that impacts our respective homeland security, yet protect methods and sources. We must learn to integrate intelligence and law enforcement information, yet protect the individual rights of our citizenry.

● (1650)

While the focus of today's homeland security has brought the threat closer to home, we must remember that the environment is not only intelligence-centric, but it is rule-of-law-centric as well. In the 21st century, where transnational crime and terrorism pose substantial and increasing threats and risks, it is worrisome for both our countries that the growing nexus between criminality and terrorism force multiplies the threats we face today.

We require a better understanding of today's and tomorrow's challenges in order to best address them, and we must move away from our past definition of those challenges. We must address the challenges in context as they are today and will be tomorrow, not as they were yesterday, for it is proactivity that shall determine our collective future successes or failures.

Your country, much like my own, was built on sound immigration policy, and ensuring these policies remain sound and go forward will be a determining factor in the positive growth of both our great nations.

In closing, both the United States and Canada have talented security and intelligence professionals to perform the work that lies ahead. These people exist both within and outside the government. It should be a priority of government to engage these professionals and use to the fullest capability the sound knowledge and practical solutions they offer to the security problems our nations face together.

We must ensure the right personnel are in the right positions. This human capacity, supported by sound and safeguarded intelligence, operating collaboratively between domestic agencies and international partners, will ensure that the legitimate traveller and the legitimate refugee are properly admitted to our countries, thus enjoying all the wonderful opportunities your country and mine have to offer.

The Vice-Chair (Ms. Jinny Jogindera Sims): Thank you very much for your presentation.

We will go to Député Opitz.

Mr. Ted Opitz: Welcome back, Admiral, and welcome back, Mr. Platsis. It's good to see both of you again.

Admiral, from your former job as deputy director, you mentioned the intelligence gathering capabilities of what you were doing, which obviously impacts military situations and the overall security of a nation, but it also impacts migratory patterns of human beings, whether it's through immigration or just travel and movement back and forth.

You discussed at length the value of intelligence. The previous speaker talked about human intelligence in particular and how some of that is gathered. From that specific point of view, you also said that human intelligence and intelligence generally has to interact with the machinery, literally, of biometrics to be able to give you the whole intelligence picture so you know who's coming and going. Could you comment on that, sir?

● (1655)

RAdm Donald Loren: Sure, I'd be very happy to comment.

One of the things we both have to deal with as nations is trying to describe and identify today's problems and our future problems and challenges in yesterday's terms. When I say intelligence, we all immediately conjure thoughts of 007, Cold War definitions, military intelligence. In our IRTPA of 2004, the Intelligence Reform and Terrorist Prevention Act, and I will quote that law as that's our own, we go to great lengths to use the word “information”.

This is where the two areas start getting very grey. We have to be very cautious in the United States, as do you, I would suspect, as to what is information, what is intelligence, what is military intelligence, what is national security intelligence, what is law enforcement intelligence. These areas get grey.

We have to learn to understand how to collect that information, whether it be from what we call open sources, from clandestine sources, from international sources, or from specific activities, and piece that information together, yet absolutely respect the rights of our citizens. The last thing we want to have are non-law enforcement government agencies collecting intelligence on individual citizens. We are constantly very cautious of that. It would violate our Constitution. It violates the ideals and beliefs we have as a nation. That doesn't make the challenge any easier.

We have to make sure there is a sharing of information. There has to be a hands-off at some period. There has to be a turnover to those who are duly vested with responsibility for law enforcement, who can gather that type of intelligence, or information, whatever you choose to call it.

One of the things we have to realize is that we cannot stereotype terms and apply them across the board. We have to be very cautious of how we use those terms.

Mr. Ted Opitz: How does the information, from a law enforcement point of view, now combine with biometric technology to create a picture for, say, a CBSA agent at the border?

RAdm Donald Loren: I listened to your former panellist's comment. I am not a biometrics expert by any means, but I do want to distance myself a bit from the use of biometrics to gather intelligence and to conduct profiling. I'm a nuts-and-bolts kind of guy. Biometrics is using the technology we have at hand to ensure you can prove who you say you are.

We've evolved throughout history. We had letters of mark, we had credentials, and then we invented photography and we were able to use your photographic image. We had to deal with cultures that thought using your photographic image captured your spirit, yet we worked through those sorts of things.

As the technology changes, I simply want to be able to ensure that when you use that government ID card and put it into your computer, and if you take your index finger and put it on the reader, I can prove that the fingerprint identification of the person using the card that has the information is confirmed and you are who you say you are, and you did not simply come by that card.

So I'm very cautious about staying away from biometrics as intelligence gathering; it's purely identification.

Mr. Ted Opitz: Thank you, Admiral.

Mr. Platsis, in terms of interoperability, of sharing information between nations, whether it's the United States and us, or the U.K. and others, and even within our own departments here, what would your comment be? You talked about the interoperability of these departments and Shared Services Canada trying to basically integrate and aggregate a lot of that information. Can you comment on that, sir?

● (1700)

Mr. George Platsis: Sure.

My concern when all different types of information are conglomerated...as I mentioned, you have differing levels of security protocol. I gave one example, that the one issue of admissibility crosses a whole level of different departments. All of these departments have differing levels of security in what they use on their internal protocols. Yes, Shared Services Canada does want to streamline. But again, it's protecting the integrity, the confidentiality and availability of that information. For example, if CIC or CBSA has information on some person and then they need to verify it with, say, CSIS or the RCMP, at some point along that line it may be possible—it may not—that the information goes from being something that's unclassified to it being a person of interest. At what point do we ensure that the information hasn't been contaminated and hasn't been altered at all?

From a biometrics standpoint, for example, yes, we can get a retina scan, and, yes, we can get a fingerprint and we can do all this, but when we actually have our electronic document, are we sure that this information has been safeguarded in a particular way?

I noticed from the previous session that you pulled out your NEXUS card. I have a NEXUS card as well. For anyone who has a NEXUS card, you'll see that you actually get this little sleeve that you're supposed to keep your NEXUS card in, because of technology that's actually embedded inside the card—it's NFC, near field communication. Lots of passports are actually starting to use this right now with e-passports....

Is that it?

The Vice-Chair (Ms. Jinny Jogindera Sims): Finish your sentence.

Mr. George Platsis: Okay.

I only want to say that we need to ensure that that information is also protected, because there have been cases to show that even electronic documents can be forged and can be manipulated.

The Vice-Chair (Ms. Jinny Jogindera Sims): Thank you very much.

I'm now going to go to Député Freeman.

Ms. Mylène Freeman (Argenteuil—Papineau—Mirabel, NDP): Thank you, Chair.

I'm new to this committee—

Mr. George Platsis: Welcome.

Ms. Mylène Freeman: —but I understand you have presented to this committee before, Mr. Platsis, on this specific study. I went to the evidence of March 15 when you were here and pulled out some questions I have from looking at your testimony.

You mentioned that the Auditor General made numerous recommendations with regard to the improvements of the integrity and security of our immigration system. He revealed that officers have no idea who should be coming to Canada, as they do not have enough specific data to make an assessment on admissibility. Additionally, there is a lack of performance reviews, guidance, and training.

While biometrics may assist with the information collection, these recommendations by the Auditor General are not addressed. Officers may still not be administering the current laws accordingly, with little oversight.

You stated on March 15:

> The situation becomes even more daunting because of inadequate ongoing training and an overreliance on technology, which risks both increased danger and complacent behaviour.

What human resource improvements should accompany the implementation of biometrics, if there were to be future legislative changes?

Mr. George Platsis: I think you mentioned in there, to use as a departure point, that biometrics should not be used as a collection point. To echo the Admiral's thoughts, it's more of a verification process. We need to know more about people before they actually show up at our borders.

There's been a little chat right now about HUMINT, and HUMINT is not necessarily, again to quote the Admiral, the James Bond type of situation. Human intelligence can range from something as simple as community engagement. For example, Canada has the most multicultural community in the world. We have everybody from every side here. We need to get some more community engagement, because if you actually think of it, global security is a function of local security, so how can we help verify this information about people coming in, engage these communities that we have?

For example, in the greater Toronto area I'm sure you could find pretty much anybody from anywhere you want. This is human intelligence that is being built up to create information, not necessarily only about a person, but, for example, a particular region, because these people call back home, they have relatives there, they have family there. It's all these little pieces of data that start coming together, so that we have a better understanding, if not necessarily of a particular person, then of the context of a particular part of the world.

● (1705)

Ms. Mylène Freeman: I find that very interesting. What could you recommend concretely for this government to do in order to engage those communities?

Mr. George Platsis: I think you could start with even local law enforcement. I have seen and know of senior law enforcement officials who have been very active in engaging diverse communities. As opposed to waiting for these communities to come and talk to us, we should be going to them and talking to them, saying, "Tell us a little bit about your part of the world."

Ms. Mylène Freeman: That's interesting.

On a related topic, you did mention a few minutes ago accuracy of information that comes from, if I'm not wrong, RCMP or CSIS, to CBSA, for instance. On March 15 you mentioned that:

> If the RCMP or CSIS has somebody on their watch list, but they do not inform CBSA, it is not the fault of CBSA that they let the individual into the country. It is the fault of the system for not ensuring that necessary agencies can easily integrate and share their information.

Better information sharing between departments was also recommended by the Auditor General. I assume you agree with the recommendation. How do you suggest we could actually have better information sharing?

Mr. George Platsis: You could say this of government and many other sectors: we suffer from institutional silos. There are both institutional barriers and there are cultural barriers. There's plenty of information that I think you can find on this in numerous research studies, that certain departments have traditionally not worked well together because there's a cultural base.

To go back to almost the same idea from the previous response, it's dialogue. Within your own institutional silo, you could probably handle your issue. But once we start crossing into different departments and into different spectrums, person A from organization A might not work that well with person B. We need to actually start chipping down these silos and getting a more inter-agency response going on.

As a function of that, we are going to start sharing a whole lot more information between each other, and the more information we share with each other, we create a larger database. The larger database that we create is something that we need to safeguard, because like most databases, they become a target; they are a risk. Unless we start chipping down these institutional silos, which could be between departments...and I would even suggest internationally, with some of our traditional allies, we need to talk a little bit more. To take a quote from one of my other fields, in disaster and emergency management, the time to exchange business cards is not when the disaster happens, it's before.

Ms. Mylène Freeman: You walked right into my next question, which is, what kind of security provisions should we have to basically ensure the safety and security of this information, if we're going to be having much more information sharing, etc.?

Mr. George Platsis: That's a long question. I'll try to give a short response.

There's both the technological side and the human side to this. For example, you can have the absolute greatest technological solution, but if you have someone, say, from this committee walk to a computer and plug in a USB key with a piece of malicious code, you have just compromised the entire system. Not only do we have to have this technological safeguard, and you can see this on numerous reports—the most recent one would probably be the CSIS one that came out last week; we are getting attacked daily. If you want me to get you some statistics on how malicious.... Do you want statistics? Okay.

Again, you have to understand that these are estimates, because not everything is reported, and these are coming from places like McAfee and Google—

The Vice-Chair (Ms. Jinny Jogindera Sims): Thank you very much. Could you finish your sentence?

Mr. George Platsis: We are attacked daily by a cyber threat. We need the technological solution and we need a human solution.

The Vice-Chair (Ms. Jinny Jogindera Sims): Thank you.

Ms. Mylène Freeman: Thank you.

The Vice-Chair (Ms. Jinny Jogindera Sims): Our next speaker is Député Lamoureux.

Mr. Kevin Lamoureux: Thank you, Madam Chair.

I will have both of you provide some comment.

One of the big issues for many Canadians—if not the majority of Canadians—is to be able to travel. Given that you are here, Admiral, I am going to focus on the United States. Whether it's cross-border shopping, commercialization, big trucks, visits, and all sorts of reasons, we have Americans coming north and Canadians going south. Part of the concern is when you look into the crystal ball and ask, "What is it going to take in order to board the plane?" For now, we'll talk about the cars crossing the border.

What do you believe is necessary in order for us to allow for that flow in a reasonable time span? Is there something specific that government could be doing that maybe it's not doing? Is there enough interaction between the U.S. Department of Homeland Security and the Canadian security services?

Given that this will probably be my only question, because there are only five minutes and both of you will respond to it, if you want to touch on the airports, that would also be beneficial.

Thank you.

● (1710)

Mr. George Platsis: To clarify, are we talking Canadian and U.S. citizens only, or are we talking at large?

Mr. Kevin Lamoureux: It's citizens of both countries exchanging across. Let's just assume they are all doing it in goodwill and are no real threat. What kind of process do we—

RAdm Donald Loren: That's an absolutely great question. It's a question that I think gets to the very heart of how our two nations need to address a continental, if not a regional—two thirds of the continent—problem or challenge. Yes, we have made tremendous progress over the years—certainly since 9/11—in cooperation and information sharing. ITAC and NCTC both work very closely. You are exactly right. This is that complicated interaction between terrorist information, intelligence, law enforcement information, and relationships between our largest trading partner.

How do we make that all work? I would suggest to you—I'm going to be a little bit cynical here and probably predicate it on only a marginal amount of fact. I would be surprised if we were to say our processes, while evolving, are all predicated on how we protected against rum runners coming across the border during Prohibition. I'm not sure I want to spend a lot of time on bona fide commercial traffic going across the border, so I'm with you. For the legitimate traveller and businessperson, we need to work to solve those relationships. The problem is, we have to have absolute transparency and understanding and the ability to control our borders from the exterior.

I would venture to say the typical resident of Ottawa and the typical resident of Washington, D.C., are not the threat coming across the border. What we have to do is make sure we have the right application of technology and processes that allow us to verify that truck coming from DuPont into Canada contains the materials that are on the bill of lading and that it's driven by a driver who has correct identification. Whatever we can do to make that easy, whether it be RFI technology, biometric technology, as well as sound, protected processes within our individual nations....

I personally believe we should work to the best of our ability to eliminate as many of the controls as possible across the northern border of my country and the southern border of yours, but that means we have to get a number of other things right first. I am not worried about the typical inhabitants of Ottawa. I am worried about people who come up illegally through my country, either to gain access to my country, or to potentially gain access to your country, or people coming in from the north or other points of entry into your country and then trying to come across an unprotected border to the north of mine.

We have to make sure we have the processes and correct interaction between agencies. Again, this gets back to the—intelligence always took place in another part of the world. Now it's law enforcement. I would venture to say—

The Vice-Chair (Ms. Jinny Jogindera Sims): Perhaps you could finish off your thought, please.

RAdm Donald Loren: —in my country, we were much better prepared to do foreign intelligence than we were when the threat came to our own shores.

A voice: That's a good point.

● (1715)

The Vice-Chair (Ms. Jinny Jogindera Sims): Thank you very much.

For the next speaker, actually, we have two for the price of one. It is Député Weston and Député Menegakis. They're going to be sharing their time slot.

[*Translation*]

Mr. John Weston (West Vancouver—Sunshine Coast—Sea to Sky Country, CPC): Thank you, Madam Chair.

How much time do we have?

[*English*]

The Vice-Chair (Ms. Jinny Jogindera Sims): Seven minutes in total.

Mr. John Weston: Okay.

Welcome both. Nice to see you back again.

I'll put in a little plug for Mr. Platsis, given that you're at my alma mater, Osgoode Hall. I wish you well there. It's rare that you get someone who's so involved in both teaching and studying at the same time. I don't know how you do it all.

I'm glad you were both here to hear the other witnesses, because I listened very closely to what they had to say. I was listening to their criticisms of biometrics, and it seemed to me that the most trenchant criticism they have is that it's not perfect. In fact, one of the last comments from Mr. Muller was that these are not infallible technologies.

Early on in your testimony, I think it was you, Mr. Platsis, who said these technologies should be a tool, not a crutch.

Can I just ask you to address the concerns that were raised in the first hour? Should we be throwing out biometrics because they're not perfect? Should we be saying that because there are false matches sometimes, therefore biometrics should not be used?

Maybe you could each spend a couple of minutes on that.

Mr. George Platsis: Do you want me to take the first crack? Okay.

No technology will be perfect. That's something the committee should understand, not only for this committee, but any study. For any technology, it's simply a function of time before it breaks down —any secure system. It could be a matter of seconds, it could be a matter of years, depending on the security infrastructure that's there.

Will mistakes happen? Yes, mistakes do happen. Of course, I'm not going to name names. I'm going to give an example of where a NEXUS cardholder, someone who has been processed by both countries, has been vetted by both countries, somehow randomly, somewhat frequently, still manages to get four S's on their boarding pass when leaving from a certain airport and not going to a particular other state. The four S's, for people who don't know, is a secondary security threat.

That's a little bit of a problem when you rely solely on the technology to be doing this.

I do not think that tossing away the benefits or the technology writ large of biometrics would be the best of ideas. It's an evolution of how we do identity, and I think the Admiral explained that quite well. We went from tombstone data to photographs to fingerprints. I think the information needs to be secured, with the understanding that it will not be perfect.

So if we're going to invest in these sorts of systems, be it information sharing between departments or biometrics, we have an inherent responsibility also to safeguard the systems, the databases, the infrastructure that they are predicated on.

Again, any sort of database—and this is a great example—becomes a target for others. So we have a responsibility, as we're collecting personal information, that while we do use it to verify and make sure that the right people are coming here, we need to protect it.

This is just my last point before I pass it over to the Admiral.

Starting a biometric file on someone or starting a file at all on someone when they just show up to our border doesn't really do much. We need to know more about the person before they actually come to us. I could just show up, for example, to the United States and give a fingerprint scan. If there's nothing to talk about—George Platsis or this fingerprint or this retina—the file starts there.

The Vice-Chair (Mr. Kevin Lamoureux): We're just going to go to Mr. Menegakis, because you actually have about three minutes left now. Is it okay?

Mr. Costas Menegakis: No, my colleague can finish.

Mr. John Weston: So no one's saying this should be done in isolation, and you both made the point very well that it should be done with human intelligence as well.

Given the NEXUS that you like to use, Admiral, between Canada and the United States, and given that together we're more able to protect against terrorism than if we try to do this in silos, then how would you put biometrics as part of that NEXUS?

And, please, maybe we'll leave a minute or two for my colleague.

● (1720)

RAdm Donald Loren: I'll do my best.

When I was growing up, my father refused to buy a colour TV until they perfected it. It's not about the technology. Who cares about the technology? Moore's law tells us that the technology is going to change in two years anyway. It's about what we're trying to do with the technology. What is the application? What are the processes that we want to employ?

Why would I ever—no offence—want to start a biometric file on anyone? I'm not sure what good that does. Again, I'm not an expert, but I do know that each of our governments has some sort of certification and documentation of who we're supposed to be, and we're just moving forward so that somehow, in today's state-of-the-art technology, it's real easy for me to put my photograph on somebody else's passport. So now I want to take advantage of the state-of-the-art technology that exists. So to sit there and say, "That is my fingerprint, my iris, my retinal scan"....

When you get into law enforcement, then we have uses for DNA samples. But now that gets very touchy, because that's intrusive. That requires giving a sample. It gets complicated. But that's law enforcement.

You need to know what you want to do with the technology. That's the critical factor, I believe.

Mr. John Weston: Once you know, once you want to keep out terrorists, then you would say—you were just pointing to your passport, and you were showing it up to the committee—that it would be a useful device, among other tools, to help us protect ourselves from the terrorists?

RAdm Donald Loren: I believe so.

Mr. John Weston: Okay.

Costas?

Mr. Costas Menegakis: I think we're done, are we not?

The Vice-Chair (Mr. Kevin Lamoureux): You have 30 seconds.

Mr. Costas Menegakis: I have 30 seconds? Okay.

Let me use my time, then, to thank you for coming here. It's always a pleasure to have you with us. This is a study on security that we're doing, so this information, this testimony, is very useful to us.

Our goal, of course, is to ensure the safety of Canadian citizens. Before we allow someone into the country, we want to identify who they are. Any tool we can use to help us in that identification process better protects Canadian society. Quite often people come here with no documentation. I'm sure you've had those experiences.

I had only the 30 seconds, so I will just say a big thank you once again before we move on to the next member here.

Thank you.

The Vice-Chair (Mr. Kevin Lamoureux): Mr. Choquette, you have five minutes.

[*Translation*]

Mr. François Choquette (Drummond, NDP): Thank you, Mr. Chair.

I want to thank the witnesses for being here today.

Border security is a compelling and important issue. However, I wanted to mention that, in Drummondville, in my riding, Drummond, many immigrants come to see me and raise other points that are also very important, such as better learning recognition and better access to the labour market. Those are elements that would facilitate integration into Canadian society. I hope that your committee will soon study those issues. They also constitute an urgent need.

As for today's topic, Mr. Platsis, you mentioned during your previous appearance before the committee that biometric information was not really useful unless it was cross-checked against a list, a database. A number of witnesses have brought up various problems with security and no-fly lists—be they internal or shared by several countries—when it comes to both the risks of mistaken identity and the difficulty in changing those lists in case of errors.

Is that a concern for you and do you have any potential solutions to recommend?

[*English*]

Mr. George Platsis: Thank you.

Concerning the comment about faulty information—I think I somewhat touched on this in my opening statement—we need to have some sort of mechanism, and it may be outside the bounds of this study, whereby we can verify our own information. In anything in life, it would be not prudent to take just one source and assume that it should be "the source". You have crossing vectors and nexuses that create a sounder picture. This comes back to the question of sound information.

Again, this may be outside the purview of this particular study, but reviewing things, for example, such as how the RCMP can manage things under the Security Offences Act, because they are the lead agency for national security, or how CSIS, under sections 12 through 17, or it might be section 18...how they collect information and what they do....

It goes back to what I was talking to Ms. Freeman about. We need to break down these institutional silos. We can't rely just on one picture; we can't rely just on one statement. With our membership in the Five Eyes, we need to be able to do something from a Canadian perspective that allows us to further this information sharing. Otherwise, every other country has its own interests—I say this respectfully of my colleague, whom I admire very much—as Canada has its own interests, and unless we can take this from a Canadian vantage point, we risk being handed information that is not necessarily in our own best interests. It may be—you would like to believe that your partners and allies are looking out for you—but at the end of the day, everyone is going to be looking out for their own interests.

I will only comment on a very quick case, as an example that is in open source, even though it wasn't detailed—it came out of the U.K. —in which the U.S. was afraid to share information about a Mumbai-style attack happening inside the U.K. for fear that their own U.S.-interest sources might be compromised in the process.

We have our departmental institutional silos and then we have our international silos. We need to be more comfortable working together, keeping in mind that if we want the best decisions for Canada, they need to be taken from a Canadian vantage point, with a Canadian verification and a Canadian assurance.

● (1725)

The Vice-Chair (Mr. Kevin Lamoureux): You have 45 seconds.

[*Translation*]

Mr. François Choquette: I think you talked earlier about the danger of having certain kinds of information, about the freedom of individuals and the sacrifice of that freedom.

Even if biometrics became the norm, I think it would be important to ensure good transparency so that people's rights and privacy are not infringed upon. You already mentioned that it was important to make sure all that information is not jeopardizing anyone's privacy. So we need to find processes to ensure very good transparency.

I will let Mr. Platsis answer this. Thank you.

[*English*]

The Vice-Chair (Mr. Kevin Lamoureux): I'll have to just.... I'm sorry.

RAdm Donald Loren: Actually, I am going to answer that question.

The Vice-Chair (Mr. Kevin Lamoureux): No, actually, we don't have any time. We will have to go to Ms. James, and Ms. James can determine whether or not she wants to repeat the question.

Ms. Roxanne James: Thank you, Mr. Chair.

I thank you both for being here. I cannot tell you how refreshing it is to have witnesses actually speak to the purpose of the study. The questions we are discussing in this last hour are all related to the study. I really appreciate both of you being here and waking me up somewhat.

I am going to ask a question straight out. Does the United States collect biometrics on all of its citizens?

RAdm Donald Loren: Absolutely not. There are certain categories, such as the military, for which DNA is collected, but—

Ms. Roxanne James: But for biometrics, there's not a file on every American?

RAdm Donald Loren: Absolutely not.

Ms. Roxanne James: That's good to know. I'm not planning to move there any time soon, but I will let you know that neither will Canada have one. The purpose of the biometrics we are moving to is for foreign nationals only.

As you have stated, there is no use collecting biometrics unless there is a real purpose for it. The purpose we are implementing is so that “who applies is who arrives”, so that we can verify that at both ends.

I am going to ask a question. You held up a fake passport and said you can change the picture very easily. How easily can someone change their fingerprint?

I am questioning this because I have heard in other sessions someone saying that biometrics is not foolproof and that it is easy to change your facial structure and easy to change your fingerprints. Is it easier than changing a document, such as taking one person's photo and putting it on another person's passport?

RAdm Donald Loren: I'm not an expert in this. I'm going to give you an opinion, a personal opinion. I would venture to say that it's probably not as easy as motion pictures might make it out to be, but I would venture to say that it perhaps is possible. I'd venture to say that in 2012 it's probably more possible than it was in 1950, and that in 2020 it may very well be easier than it is in 2012. That's why we go through, in the United States...is it thumbprint, index finger, five-print, ten-print...? We constantly evolve—

● (1730)

Ms. Roxanne James: I was waiting for that word—

RAdm Donald Loren: Yes.

Ms. Roxanne James: —because it certainly sounds like an evolution of technology.

RAdm Donald Loren: But in the same vein, if you really want to circumvent the system, then I'm going to ask for ten prints, I'm going to take a retinal scan as well, and then hopefully, as perfected, I'm going to do cheekbone measurement as well. You're really going to have to go to some effort to change all of those things.

Ms. Roxanne James: Thank you.

We had a couple of witnesses mention the infamous Richard Reid, the shoe bomber. They talked about the problem with profiling. Apparently this person fit every profile that should have raised all the bells and whistles, and in fact it did, but he was still allowed to board a plane.

Now that we know who he is...and if he had provided biometrics at some point after he was arrested, charged, and convicted, would he be able to easily walk into your country if you were also using biometrics and he popped up in your database as being the shoe bomber?

RAdm Donald Loren: Well, that gets back to the previous question: would it be easy? I don't think so. Would it be infallible? Of course...it could be fallible. It's not infallible.

The Vice-Chair (Mr. Kevin Lamoureux): At this point we're going to adjourn the meeting. The bells are ringing and it's 5:30.

Thank you for your presentations.

The meeting is adjourned.

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

SPEAKER'S PERMISSION

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

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

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

PERMISSION DU PRÉSIDENT

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

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