HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Citizenship and Immigration

CIMM • NUMBER 049 • 1st SESSION • 41st PARLIAMENT

EVIDENCE

Tuesday, June 19, 2012

Chair

Mr. David Tilson

Standing Committee on Citizenship and Immigration

Tuesday, June 19, 2012

● (1530)

[*English*]

The Chair (Mr. David Tilson (Dufferin—Caledon, CPC)): Good afternoon, everyone. This is the Standing Committee on Citizenship and Immigration, meeting number 49, Tuesday, June 19, 2012.

This meeting is televised and is pursuant to Standing Order 108 (2). We are studying “Standing on Guard for Thee: Ensuring that Canada's Immigration System is Secure”. In other words, it's a study of the security of the immigration system.

We have some guests who are appearing before us for the first hour. There are two groups. From Defence Research and Development Canada we have Pierre Meunier, who is the manager of surveillance, intelligence, and interdiction, Centre for Security Science. Good afternoon, Monsieur Meunier. From NextgenID Canada Inc. we have with us the senior vice-president of corporate and business development, Robert L. Bell. Good afternoon, Mr. Bell. Finally, also from NextgenID we have Ilan Arnon, vice-president of technology solutions. Good afternoon to you.

Each group will have up to ten minutes to make a presentation. Then members of the committee will follow with any questions they have, and I'm sure they will have some.

We will start with Monsieur Meunier.

Mr. Pierre Meunier (Portfolio Manager, Surveillance, Intelligence and Interdiction, Centre for Security Science, Defence Research and Development Canada): Thank you.

My name is Pierre Meunier, and I am the portfolio manager for surveillance, intelligence and interdiction at the Defence Research and Development Canada Centre for Security Science. This portfolio includes leading a community of practice on biometrics for national security.

I would like to provide you with an overview of who we are, what we do, and our relationship with federal government partners and the broader public safety and national security community. I will then provide you with a brief outline of some of the work we've invested in surrounding biometrics and what expertise we can contribute to support the exploration of biometrics technology in Canada.

The Centre for Security Science was established through a memorandum of understanding between the Department of National Defence and Public Safety Canada and is managed by the Defence Research and Development Canada special operating agency under the Department of National Defence.

The centre's mission is to pull requirements and priorities from the policy and operational communities and task the science and technology community and government, industry, and academia to develop solutions and provide advice that addresses these priorities.

The centre's staff includes scientists and engineers with a wide range of relevant experience who also possess expertise in areas such as capability-based planning, risk assessment, operational research, knowledge management, project management, community-building, and the application of scientific methodologies. They are therefore well positioned to provide trusted advice.

Over the years the Centre for Security Science has built a network of experts it can draw upon to serve the needs of the federal government and the broader public safety and security communities.

Through hundreds of projects and activities the centre and its partners have improved Canada's capabilities, ensuring that responders, planners, and policy- and decision-makers have access to the scientific and technical knowledge, tools, processes, and advice they need to protect Canada's interests.

As mentioned, one of my roles as the portfolio manager for surveillance, intelligence, and interdiction is to lead the Biometrics for National Security Community of Practice. It's important to note that as a portfolio manager, my role is to oversee projects and activities that foster collaborative efforts among experts. I'm not a leading-edge technical expert in any individual biometrics technology per se. However, my engineering and scientific background, combined with my interactions with national and international partners, has allowed me to gain an appreciation of how all the pieces of biometrics security fit together.

The Biometrics for the National Security Community of Practice brings together key stakeholders from federal departments and agencies responsible for national security, law enforcement, and immigration to discuss and study technical issues surrounding the use of biometrics technology in Canada, as well as to identify and address capability gaps.

To date this community has undertaken a number of biometrics studies looking at the performance of various technologies in different operational settings and examining privacy protective measures. In addition to these studies, experts have come together on a number of occasions to discuss issues and to raise awareness of what different departments are doing in this area and to share best practices. These discussions provide valuable knowledge and guidance for future investments to support the further development of this capability.

DRDC also has experts in systems engineering, including skills and knowledge in areas such as design testing, data management, and pattern recognition, all of which can be applied to understanding biometrics systems. Bringing this type of technical expertise to the table is what the Centre for Security Science can offer to support departments and agencies responsible for national security, law enforcement, and immigration in making decisions surrounding the technical requirements and performance factors of biometrics.

Thank you.

● (1535)

The Chair: Mr. Bell.

Mr. Robert Bell (Senior Vice-President, Corporate and Business Development, NextgenID Canada Inc.): Mr. Chairman, and honourable committee members, we are pleased to appear before you on this important study examining the security of Canada's immigration system.

As someone who has been active in the field of biometrics for close to a decade, I will begin my remarks by noting how encouraging it is to see that biometrics are specifically included as one of the subject areas in your study. The realization that biometric identification technology has an integral role in immigration strategies is, in my view, significant.

NextgenID has worked with a number of governments at initial stages to help them determine if they should use biometrics, and if so, which biometrics they should use for passports and for border control. We have then participated in delivering technology and systems to help these countries implement face and fingerprint biometrics for passport, visa, and national ID issuance, as well as for border control.

My colleague Mr. Ilan Arnon has been the key technical person on many of these projects, and he will be able to answer your questions, given his first-hand experience on such projects around the world.

I'll begin by discussing examples of security gaps and some specific opportunities to deploy biometrics to strengthen our immigration system.

Deploying the right biometrics in the right applications will unquestionably both improve the security of our immigration system and expedite the clearance of legitimate travellers. Our work has been focused on systems for face recognition, fingerprints, and iris biometrics, which I would suggest are the only biometrics suited to the identification requirements associated with immigration and border control. Any system such as that seeks to verify identities and detect persons on a watch list.

I would like to address three specific security gaps that can be filled in part through the use of biometrics. One relates to visa issuance. The second relates to identity confirmation at the border. The third is a bad-guy lookout at the border, basically surveillance, looking for faces, and seeing if those people are on the bad-guy list.

With regard to visa issuance, the government is currently planning to capture fingerprints and face images during the application process. This isn't in place yet. This is just under initial contract at this point, as I'm sure you're aware. These fingerprints will be used as the biometric to confirm the identity of the traveller on arrival. So if you issue the visa, you make sure that the person who's coming to the border is actually the person he says he is.

This is a commendable first step. However, I would suggest three ways in which this could be improved at a relatively low incremental cost. Given that the face has been captured, facial recognition can be used to check if the applicant is on Canada's bad-guy list. Remember, for a known terrorist there will probably be a photograph, but it's unlikely there will be a fingerprint on file. A face can be captured upon arrival, and facial recognition can then be used to confirm the identity of the visa holder.

Review of a possible match can be performed immediately by an immigration officer with minimal training, unlike the case for fingerprints, for which you need an expert. If a potential face match is found, then fingerprints can be used as an alternate biometric during a secondary check. That's for visa issuance.

The second item is identity confirmation at the border.

When a person arrives at our border, he or she is either known or unknown. Known travellers have been pre-screened through the visa application program or the trusted traveller program. A trusted traveller simply has to confirm that he or she is the rightful holder of the passport. Iris recognition is used for trusted travellers, and as noted, fingerprint is planned for use for visa travellers. Canada is looking to extend participation in the trusted traveller program, CANPASS and NEXUS.

Beyond that, the advent of e-passports will make the use of biometrics to screen all travellers possible and practical. For example, in Australia, at all airports, the e-passport is read, and then a live image is captured and compared with that on the e-passport to determine the authenticity of the traveller. New Zealand and a number of European countries are moving in this direction as well, so they're automating their processes. This means that a good forged document will not be sufficient to gain entry into Canada.

● (1540)

This approach is also leading to automation, using e-gates at the border to quickly screen low-risk travellers and to enable the immigration officers to focus on the high-risk individuals. Canada should be planning to use this approach for e-passport holders from the U.S. and visa-waiver countries. Canada will start issuing e-passports this year. The other countries have been doing so for some time.

A following step would be to then effectively extend the border perimeter by conducting the same identity verification checks at the point of embarkation or before. Let's know who they are before they get on a plane that's coming to Canada.

The third item I want to deal with is what we call “bad-guy lookout”. Currently at our border control positions, there are video cameras deployed to capture and record the passage of travellers through the border. This provides a good record to support an investigation if there has been an incident at the border. However, it does not support facial recognition or watch-list checks that would allow a proactive response.

With the creation and maintenance of a watch list of persons of interest, these same cameras, perhaps with different camera lenses or positioning, could also act as face recognition cameras. The face images could be captured and compared against the watch list. If there is a potential match, this could be reviewed or adjudicated by the officer at the border post or at a central location, and a traveller could be sent to secondary inspection if required. If cameras are set up for identity verification, as mentioned earlier, then of course the same captured face could be used for a watch-list check.

I've been talking about face recognition. Why face? For these applications, face is the best biometric. In some cases it's the only biometric that would be effective. For identity verification at the border, the face is the only mandatory biometric on the e-passport, so it is the only biometric that can be used for the over 100 countries that will be issuing e-passports by the end of the year. For bad-guy lookouts, face is the only biometric for which there is likely an available image to verify against, and the only biometric that can be easily captured at a distance. Face recognition works well, and has been proven to do so in countries around the world for the applications recommended.

I guess the question is that we've talked about technology, but is there a problem? I think it is clear from the press—and I think you people would probably know better than I—that there are significant numbers of persons who commit crimes in Canada, are arrested, charged, tried, and convicted of these crimes, and then deported, only to come back under another identity to do that same thing again. On the CIC website there are five examples of people who have been deported for serious crimes, only to return—some three times, one 17 times—as repeat offenders. They come back, they commit crimes again, and they're removed from the country. This is a cost to society that can be largely eliminated with the proposed bad-guy lookout.

Mr. Chairman, let me close my remarks by noting that as someone who has worked in the industry for years, I am greatly encouraged when I see studies such as the one this committee is undertaking and initiatives such as Bill C-31, which expressly authorizes taking biometrics and enabling what is in effect the bad-guy lookout system at the border. What categories of person should be included in such a bad-guy database is a policy decision for government to make, but it is important for you that you appreciate how the technology itself supports such efforts.

Canada is clearly moving towards the screening and security approach in the Canada-U.S. border agreement and in our recent adherence to the five-party conference—Canada, the U.S., the U.K., New Zealand, and Australia—on biometric data sharing to prevent immigration fraud. Biometrics is a technology that can significantly enhance the security of our immigration and border systems, while also expediting the clearance of legitimate travellers.

I hope these opening remarks have been of assistance. I look forward to any questions you may have on the subject.

Thank you.

● (1545)

The Chair: Thank you, Mr. Bell and Mr. Meunier. Your comments have been helpful. We appreciate you bringing in your expertise to help us with this report in order for us to give some comments to the House of Commons.

The first person to ask you questions is Mr. Menegakis.

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

I want to begin by thanking you for being here and testifying before us today.

This, as you can well appreciate, is a very important study for us, and a very important initiative. We feel, as a government, and let me just say as a Parliament, that it is our responsibility to ensure the safety of our Canadian citizens. Certainly it is critically important for us to identify individuals prior to their entering our country, living in our neighbourhoods, going to school with our kids, and shopping where we shop. It really has become an increasing concern, given the creative ways those who would participate in illicit activity can find to enter our country—by many accounts one of the most welcoming countries in the world in which to live.

I have a number of questions for you. First, in your opinion, under our current system how successful has Canada been at preventing criminals from entering our borders from source countries?

My questions are to all of you. I wouldn't mind hearing from all or some, as you wish.

Mr. Robert Bell: I think that's sort of a government question.

Mr. Pierre Meunier: I'm afraid I don't have an answer to that. It's not appropriate for me to comment. We're focusing on the technology aspects that could be brought to bear on this in the future or in the near future; we're not looking at the past performance issues.

Mr. Robert Bell: The thought I have is that we do a lot of work around the world, and I see each country struggling with how to make our borders stronger. As I speak with people, they have countless examples of gaps in their system, just as I talked about here. I think everybody around the world is struggling to tighten those. Some are further ahead than others.

We don't carefully screen the people who are coming in from a face recognition point of view. I think one can also look at exit controls. I don't think we have any exit controls. So part of what we'll get to in the "Beyond the Borders" initiative, at least on the U. S. border, is some exit control as well.

● (1550)

Mr. Costas Menegakis: Thank you.

Did you want to add anything, Mr. Arnon, or are you okay with that?

Mr. IIan Arnon (Vice-President, Technology Solutions, NextgenID Canada Inc.): The only thing I could add, to follow up on what Robert just said, is that we don't do anything at the moment to capture any kind of biometric, and really it's a simple process. Someone has to cooperatively look at a camera, let's say, to capture a simple image, which everyone knows how to do. It's simpler than a fingerprint. A fingerprint's the next step, maybe, but even just to capture a facial image....

As Bob mentioned in his remarks, there is a camera currently at every immigration desk. It's not being used to capture faces; it's more just to surveil the area.

So there are some simple things that can be done to take a big step in enhancing the feasibility of biometrics.

Mr. Costas Menegakis: On the issue of biometrics, we've heard from a number of witnesses here on this committee, and it's been described by several as a 21st-century identification tool. It seems to be pretty accurate, and a lot better than the current system that we have now.

Do you think biometrics should be collected only for temporary resident visas, or should they be used for everyone entering Canada? What are your thoughts on that?

We can start with you, if you like, Mr. Meunier, and then we can continue.

Mr. Pierre Meunier: I certainly believe the technology has improved to the point where it can handle large volumes. The accuracy keeps improving. The technology is just at that stage now where it's ready for use, and other countries have realized that.

I think we are getting into that direction. I look at what Citizenship and Immigration Canada is planning in the years ahead, and I think biometrics will go a long way in helping.

Mr. Robert Bell: One of the things I see as we've been going through helping people move to an e-passport is that once you have e-passports, you place the passport on the reader and take the picture, and you have confirmed the identity. Then when I'm coming across the border, you don't have to ask me all these skill-testing questions to see if I really am the person I am. I've proven it.

I think I'd be happier, as a person, if I just did that and were able to go through. It leads, then, to automating the border such that low-risk passengers and travellers can go through the border easily, without even going through a staff location.

If you looked at biometrics for everybody, you'd want to do it so that it was facilitating and speeding up the process rather than for a security point of view. Those are the two things we end up doing with biometrics: facilitation and enhancing security. You get both.

Mr. Costas Menegakis: Mr. Arnon, do you care to add something?

Mr. IIan Arnon: In any immigration area, airports are similar. There is a lot of capture of imagery through surveillance cameras. And while those images are not necessarily of the quality needed for biometrics or facial recognition, we are capturing a lot of images. Just to go the small extra step of capturing an image that we know is going to be usable for biometrics will serve to add a lot of security.

The Chair: Thank you.

You have about 20 seconds. You can say goodbye.

Mr. Costas Menegakis: Thank you very much, Mr. Chair.

The Chair: We'll go to Ms. Sims.

Ms. Jinny Jogindera Sims (Newton—North Delta, NDP): Thank you very much.

Thank you for your presentations today.

As you know, with respect to biometrics, we have expressed some concerns in the past with regard to privacy issues, and they still remain a major concern for us. One of the documents we asked the government to provide for us, and I'm sure my colleagues remember, was a privacy impact statement for Bill C-31. I think we are still waiting for that, in one way or another. It would be good to get a copy of that report, even though Bill C-31 has passed us by.

When we met with Privacy Commissioner Jennifer Stoddart, this is what she had to say:

> As the honourable members certainly know, the Privacy Act imposes obligations whenever the federal government gathers personal information. Federal agencies must ensure certain safeguards, must limit secondary use, and must list their data holdings publicly, irrespective of the citizenship of the individuals involved.
>
> Also, should any legislative or regulatory changes be made to the immigration system, I would expect to receive detailed privacy impact assessments from the appropriate institution.

We know that the Senate has begun its hearings on Bill C-31. And we're certainly hoping that at least in that other place they will be provided with the privacy impact assessments as they are going through the hearings, even though we didn't have them.

I have brief questions, but I'm going to give them to you a couple at a time.

When the government outsources the collection of biometric data to private companies, such as NextgenID, what is done to ensure that Canada's privacy laws are being respected?

Second, how is the data retained and stored, and how many people would have access to it?

● (1555)

Mr. Robert Bell: Let's go back to the preamble, where you were talking about the Privacy Commissioner.

It is an essential component in any country we go into that we and our customer work with the privacy commissioner to make sure we are meeting the laws of the country, so that what you're expecting regarding the implementation of biometrics and what she's asking for are consistent with what we see elsewhere.

When we put a biometric system in place, we provide the system but the government owns the data. We really separate the technology for collecting the data from the data itself. The government usually is the one that has access to the data, manages the data, and sets the policies for retaining and expunging the data. It is really not a private contractor's role, and our role would be similar to any other contractor's. It is really our customer's role.

Ms. Jinny Jogindera Sims: So basically you're saying that has nothing to do with you because you only provide the technology. It's the government that—

Mr. Robert Bell: It's the owner of the system, the operator of the system, who I think in this case would certainly be the CBSA, someone who's charged with the security at the border.

Ms. Jinny Jogindera Sims: Okay. Thank you.

I'm going to ask you the next question, and you may have a similar answer, so I'm prepared for that. Which internal and external sources could this information be used by or disclosed to?

Mr. Robert Bell: What we have seen is the government's put in place a very solid firewall around the information they're gathering and controlling access to.

Ms. Jinny Jogindera Sims: So what firewall do we have that you know of?

Mr. Robert Bell: To a large extent, Canada is not collecting biometric data; they are collecting surveillance information. I don't know the answer to the question.

Do you know the answer to what we do with policies for surveillance information?

Mr. Pierre Meunier: No, I'm afraid not.

Ms. Jinny Jogindera Sims: I think for me it goes to the next stage, because here we're pursuing the use of biometric data for visas, the three categories you talked about. So obviously we're looking for answers to those questions, and I'm hoping a different witness will be able to provide us with those answers, because they're very specific.

The Chair: Don't look at me for answers. I'm just like you and learning what's going on.

Ms. Jinny Jogindera Sims: I understand you provide the system, and you don't provide how the system is managed. So I'm sure your answer is going to be identical for the next one. You don't know how long the data will be kept and when the data will be destroyed. For example, is it only for identity verification, and as soon as identity has been verified the data will be expunged, or once the tourist leaves?

● (1600)

Mr. Robert Bell: Again, it is the government's policies that we would follow, and we would set it up. Our technology is flexible. For some implementations that we do for identity verification it's exactly as you've described. You verify the identity and the data is expunged.

In other cases, people say they want an entrance record and an exit record from the border, so that information is retained for a period of time to support investigations if there are incidents that are subsequent.

Ms. Jinny Jogindera Sims: Let me just be clear. For example, I lived in India up to the age of ten—just so it's a real example.

The Chair: You'd better hurry; you've got 15 seconds.

Ms. Jinny Jogindera Sims: Okay.

So once I arrive and my biometrics are taken, I have no guarantee when they will be expunged.

Mr. Robert Bell: I think the policy should be publicized. Whatever the government policy is in other cases, it's always been publicized in terms of we will keep this data under these circumstances for this long, and I would expect that the Government of Canada would do exactly that.

Ms. Jinny Jogindera Sims: I'm really looking forward to that policy.

The Chair: Thank you.

Mr. Lamoureux.

Mr. Kevin Lamoureux (Winnipeg North, Lib.): Thank you, Mr. Chair.

I want to get right into what the government is proposing to do—we need to be very clear on this—which is to move towards biometrics in dealing with temporary visas. So that's visiting visas, working visas, and so forth. My understanding is that what they're talking about when they think of biometrics is the live picture and the fingerprints. Is that a fair comment, to the best of your knowledge?

Mr. Robert Bell: It's partly correct.

What they're doing, as I understand it, is they capture the live face image when you go to apply for a visa, they capture your fingerprints, and then they store the picture and they use the fingerprints as the biometric for matching.

Mr. Kevin Lamoureux: Okay.

So in the future, because they're doing it in a couple of ways, anyone who's going to be receiving a visiting visa or a working visa or a student visa is physically going to have to go down to some form of a government agency in order to get that picture taken, in order for that picture to be effective. Was that a fair assessment? Because you couldn't just go to the old camera shop here and then say “Here's the picture I had taken”. You'd have to go to that government-sanctioned agency, correct?

Mr. Robert Bell: Since you have to go in person to give your fingerprints, it's very easy to also get your face image captured at the same time. So you will have to go to a specific location.

Mr. Kevin Lamoureux: Right.

Today you're not required to go to an embassy or an immigration office. You can do it via courier, for example, and that's quite often done. So with this change in policy, in order to be effective for biometrics, we need to be clear that they will have to go to a government agency of sorts, ideally the embassy or a consular office, to implement an effective biometric program. Is that correct?

Mr. Robert Bell: I believe that's the case. Some countries, though, are establishing relationships with other countries. I believe the five countries I mentioned—the U.K., U.S., Australia, New Zealand, and Canada—are cooperating and will have similar standards, so it may be possible for you to go to one of those other locations as well. That will give you some diversity, some places where if Canada's not represented, perhaps the U.S. is.

Mr. Kevin Lamoureux: At the very least, in terms of when you think of biometrics, it has to maintain the live picture and the fingerprints?

Mr. Robert Bell: Yes.

Mr. Kevin Lamoureux: What about the idea of the iris scan? Do you see that being implemented shortly? Is that something that's about five years or two years away? Has there been any discussion?

Mr. Robert Bell: As I understand it, there is a provision to have iris as an alternative biometric on your passport. For the e-passport, the only mandatory biometric is face. So most countries are just putting the face image on the chip. The European countries are putting fingerprints. I know of no countries that are planning on putting iris on at this time.

● (1605)

Mr. Kevin Lamoureux: Does Canada even have the capacity to be able to do iris scans? When you think of the offices abroad, they would all have to have proper capital equipment. Is that something that's even...?

Mr. Robert Bell: It would be possible, and it's not that expensive. If you're going there, we make a product that captures face, fingerprints, and iris. So it's not impossible.

Mr. Kevin Lamoureux: In terms of the cost, I'd ask for your guesstimate. What should the cost be of being able to get a fingerprint and a live picture, if the government wanted to be able to charge for that?

Mr. Robert Bell: That's such a good question, and I wish I had a direct answer. Can I come back to you?

Mr. Kevin Lamoureux: By all means.

I think it's important to recognize that the changes the government is making are going to have an impact in two ways on an individual's ability to acquire one of these temporary visas: one is that there is a potential cost that has not been debated; and the other is that there's going to have to be that physical presence.

I wanted to get that on the record, because that is something that has not been talked about to date.

Mr. IIan Arnon: Could I add something to that?

Of course if you're going to capture fingerprint or iris, you have to go physically to the office of enrolment or the consulate, etc. But there is an option to submit electronically, if you're just going to capture face. With today's electronic cameras there are ways of automatically verifying that the image meets a certain quality standard to make it usable for facial recognition.

The Chair: Thank you, Mr. Arnon.

Mr. Opitz.

Mr. Ted Opitz (Etobicoke Centre, CPC): Thank you, Mr. Chair, and thank you to our witnesses.

In fact it all exists now. I've got a NEXUS card, and it didn't cost that much. I think it was about $50 U.S. to process this at the time. I got my fingerprints scanned without ink, just on an electronic scanner, the iris scan, and the photograph taken.

To your point, Mr. Bell, this is providing me with a tremendous amount of convenience getting through the airport lines fairly quickly, because this is a trusted traveller type of program. It does provide a lot of benefit to a lot of people who travel frequently and go between various countries. I found this to be an invaluable tool.

By the way, thank you all for coming, and DRDC as well. I worked with them peripherally in the past in my military days, and they're a tremendous organization that does some great scientific work on behalf of Canada. A lot of great work comes out of there.

I know you guys are leading-edge technical folks who are coming up with a lot of these innovations that will help keep Canada safe in the long run. And as many of us have discussed, one of the reasons we're talking about biometrics is from the security standpoint.

Mr. Meunier, you said you're the portfolio manager for surveillance, intelligence and interdiction, so you're working on biometrics from essentially a national security point of view, so I'm going to start with you, sir.

Overall, what is your opinion of biometrics and its effectiveness as a tool to prevent fraud and either apprehend or keep out of the country security threats of varying levels?

Mr. Pierre Meunier: There are a number of aspects to the effectiveness of biometrics. There's the policy side of things. There is the technology side of things. There are the standard operating procedures that one might use to control the flow of people and provide the interdiction and get the intelligence and get a system to work as a whole with the various departments that do the collection of biometrics.

The best example I've seen so far is that of our neighbour to the south. They have invested a lot in the development of biometrics. We owe them a great debt for that, because otherwise the technology wouldn't have evolved as quickly. They've also provided a model for us to follow in various aspects, integrating databases of the Department of Defense, Department of Homeland Security's US-VISIT, and the FBI. We saw that model in action in a recent visit to eight agencies in the U.S. that collect and manage biometrics. I was very impressed. It does work. It works very well. It's a matter of implementing the right policies and procedures, in my view.

● (1610)

Mr. Ted Opitz: When you observed that system, did they talk about the numbers of security threats or some sort of quantifiable indicator of its effectiveness against security threats?

Mr. Pierre Meunier: Oh, yes, indeed. There was a whole list. If you want to talk to the folks in the US-VISIT program, they can tell you how many thousands and hundreds of thousands are refused access or refused work. Once the system is integrated like this, it works very well and it's effective. My assessment is that it was very effective.

Mr. Ted Opitz: What do you think are still some of the specific deficiencies that exist here with regard to the identification of foreign nationals? Would you make any recommendations to CIC and CBSA?

Mr. Pierre Meunier: I would not make recommendations as such to CIC. I think they're definitely on the right track. They've been at it for a number of years. They've done a good job, in my view, of integrating the pieces they need.

I can't comment on the policies or the standard operating procedures. I'm just looking at the architecture and the various components they bring together. All the elements are there. In Canada we may be a little bit late out of the gate in using biometrics, but that give us an advantage, in that we're starting from the second or third generation, if you will, and ramping right up to a high level of technology.

Mr. Ted Opitz: When you were in the States you saw the electronic travel authorization, the entry and exit with the perimeter agreement. Would you agree that will be an effective element in making sure our borders on both sides are protected?

Mr. Pierre Meunier: My opinion and my feelings are that it will be.

Mr. Ted Opitz: It's an opinion, sure.

Mr. Bell—just quickly, because I think I'll run out of time soon—in terms of the equipment and development of equipment and economy of scale, my honourable friend mentioned the overall costs. When you develop this equipment and it gets widely distributed, would you agree that then any costs associated with it will tend to go down, based on distribution, use, and...?

Mr. Robert Bell: Certainly. I think that the costs of the individual sensors are low. A camera is about $500. You're looking at devices that cost $1,000 to $2,000 to capture fingerprints. So you're looking at quite inexpensive devices. We're not looking at a lot of border points in Canada. Would 600 be a good estimate of the number?

Mr. Ted Opitz: Yes. So it's very relative. The capital cost of it all is fairly low, given the numbers of years it would be in service.

Mr. Robert Bell: I think so. I did actually do estimates for the deployment of face recognition through each of the border locations. It was a surprisingly low number for a national rollout of technology.

Mr. Ted Opitz: Thank you.

The Chair: Thank you.

Monsieur Giguère.

[*Translation*]

Mr. Alain Giguère (Marc-Aurèle-Fortin, NDP): Mr. Chair, my questions basically have to do with a practical issue. A security system has to ensure that we can monitor people who enter and leave, and that the person who enters with one document and one identity does not leave with another identity and another passport.

Even here in Canada, we have the so-called “real fakes”. Those are refugees who go to an Immigration Canada office, apply for a passport with a fake birth certificate and a fake driver’s licence, and receive the document.

One of those “real fakes” crossed the Canadian border and was intercepted at the American border in Seattle. He was getting ready to set off a bomb. Will our system be able to protect us against something like that? Will it be able to tell us when someone enters and, most importantly, when they leave? If they don’t leave, will a little red light go on and tell us that someone has entered Canada illegally?

● (1615)

[*English*]

Mr. Robert Bell: Those are very good questions.

You need integrity in the process all the way through. In one project we're working on right now.... The first thing to do is make sure that when you're issuing that secure document, you actually have real, authentic breeder documents. For example, is the driver's licence that is being provided an authentic driver's licence or not? There's quite a lot in the way of security features on that driver's licence. They can be easily authenticated—or not. If you're using a passport as a breeder document, you can authenticate the breeder document as a passport.

So if you take care to make sure first of all that the person can clearly say that he is who he is, and then you capture the biometrics so that you link those biometrics to that identity, then you've made a big step. Then, when that document is presented and the biometrics are authenticated at the border, we can tell whether that's the person or not.

We're helping to solve the problem of false documents and we're also helping to solve the problem of someone using someone else's document.

[*Translation*]

Mr. Alain Giguère: Will you be able to guarantee that someone who enters Canada on a specific date is registered, and that a follow-up will be done to find out if the person left the country or not?

[*English*]

Mr. Robert Bell: The follow-up is a very important question. Right now in Canada I don't believe we have exit controls—

[*Translation*]

: Mr. Alain Giguère There isn't one.

[*English*]

Mr. Robert Bell: —and if we don't have exit controls, then someone comes in and we don't know if they go out. In other countries where we're working, they're actually taking pictures and capturing the images of people coming in. Then, as the people go out, they're checking that face image again to see if it's the same person who came in. Other countries are facing this problem. We have not yet done that.

Mr. Ilan Arnon: I just want to point out that there's one other thing that can be checked. As someone exits, you can verify that the person is the rightful holder of that document or that the person who entered on that document is indeed the same person who left or is leaving on that same document. So you can guarantee that there is no fraud upon entry and then upon exit.

[*Translation*]

Mr. Alain Giguère: I have one final question about data entry. You are dealing with five governments, but I assume that the Interpol is also involved for international warrants, and the UN for no-fly lists. I am also thinking about the different justice departments that do not allow people to leave the country with a child, in other words family abductions.

Once all that information is obtained, will you be able to make the situation more secure and prevent family abductions? Can you guarantee that all the information gathered will be secure and will not be available to the public at large? There are some very skilful hackers out there.

[*English*]

Mr. Robert Bell: Very true.

I think the example of family kidnappers is a good example to work with. If someone reports that a child is kidnapped, this would then be a flag to capture that child's face image, and perhaps the parent's face image if that's who you suspect, and then on the exit control have cameras looking for those people. It would be very effective.

Can we guarantee it? Probably not. Can we do very well? Yes.

The Chair: Thank you.

Mr. Leung.

Mr. Chungsen Leung (Willowdale, CPC): Thank you, Chair.

Welcome, gentlemen, to this hearing.

Canada is a multicultural country and we have people coming in from all over the world. My question has more to do with the level of cultural sensitivity that is built into the system and how we address some of these issues.

For example, people from Muslim countries could come in with names like Mohammad Mohammad Mohammad. The name and the surname is the same. You can have people with names like Osama, which is a Japanese surname as well as an Arabic surname. You could have 18 million Mr. Dungs coming in from China.

In some of the Asian countries I've been in, they use biometrics, in addition to matching the original national language, whether it's Chinese or Arabic, with the English translation, which can vary over time. There are other cases, like Mr. Lee, which is common to Chinese, Korean, and English surnames. Another great one is the Mr. Singhs, who are all over the Punjab.

If a person comes into Canada with that name, and he goes back and switches that with another person, how culturally sensitive are we to identifying potential abuses, as well as being culturally sensitive to the fact that there are a lot of potential errors that can surface from the complexity of dealing in multiple languages?

● (1620)

Mr. Robert Bell: There are a number of questions embedded in that.

We started with cultural sensitivity. In the case of face recognition, if that's your primary biometric for crossing a border, and if in a Muslim country they don't wish to have their face image taken, we would usually have an alternative for the person to provide a fingerprint. We would still match that person from who they say they are to a biometric, but the cultural sensitivity would be that they have a choice.

The nature of your other question was people with the same name —

Mr. Chungsen Leung: Switching documents.

Mr. Robert Bell: That's right. Switching documents is common, but once you match the document to the biometrics, face or finger, you can't switch the document without being found out. As soon as you put your passport down and take your picture or your fingerprint, the discrepancy shows.

With e-passports—and almost all countries, a hundred by the end of this year, will have those—the biometrics are embedded in a chip. It's very difficult to change that if you're forging a document. I think you really have a big step forward in the ability to verify that the person you're dealing with is the person they say they are, whether their name is the same or not.

The last one was all of those different spellings of Mohammad. Most countries we see have an ability to search on 112 spellings of "Mohammad". I don't know if Canada has that, but I do know the U. K. does.

Mr. Chungsen Leung: Within the technology that's available to you, at least the software, if someone comes in with a name like "Mr. Leung", there are probably five variations of how you can spell that, and you are able to spot that and then match that to an appropriate fingerprint.

Mr. Robert Bell: I can speak for the U.K. system. The way the U. K. system works is that if there were a mismatch between the biometric and the spelling of the name, they would check the other potential spellings of the name just trying to avoid confusion and to facilitate the travel.

Mr. Chungsen Leung: Thank you.

The Chair: Thank you.

Ms. James.

● (1625)

Ms. Roxanne James (Scarborough Centre, CPC): Thank you, Mr. Chair, and thank you to our guests.

I actually found it interesting, Mr. Bell, because a lot of what you talked about were things that actually came out in our previous work on Bill C-31 with regard to biometrics and security in this country. You hit the nail on the head when you said that we're lacking a lot of exit controls in this country, and also about the fact that we need to make sure that who applies is who arrives, and who arrives is actually the person they say they are. So I really appreciate—

Mr. Robert Bell: And if they leave.

Ms. Roxanne James: Absolutely. So I appreciate your comments, because it really stresses the importance and the need we have here in Canada to move forward with biometrics for the safety and security of our citizens.

As well, I noted that you mentioned that countries like Australia and other countries we are compared against are in so many ways actually further ahead than we are, and we're actually playing catch-up right now. So I really appreciate your comments on that.

I'm going to ask you some questions regarding identity fraud. I think I know what your answer is going to be, from your testimony, but I just want to hear it again. In your opinion, right now how capable is our government in Canada in detecting multiple, stolen, or mistaken identities? I know you talked about someone who has come back into the country 17 times, so I'm pretty sure I know what your answer is going to be, but could you elaborate on that, please?

Mr. Robert Bell: I have no first-hand experience. I can only judge the system based on what I read in the newspapers. But I do see that there is a gap. I've seen newspaper articles that say that someone has left and has come back and they were let in and CBSA said that was because they had very good documents. I think the officer is doing the best he can. He is looking at that and says that's a very good document, but he doesn't have the tools he needs to be able to make a better judgment.

Ms. Roxanne James: Absolutely. I appreciate your answer on that.

Overall, what do you think the impact is on Canada, and on the security of Canadians in this country, of not having those measures in place right now? If we were to delay this for whatever reason, what do you think the impact will be on Canada as a whole, and on our security?

Mr. Robert Bell: Of course it's unknown, isn't it? We just don't know who is coming across our borders. We just don't know when and how we're going to have a problem. I don't think there's a good answer, but it's a worry.

Ms. Roxanne James: I agree with you, I think it is a worry. I know my constituents in Scarborough Centre would also be very concerned about this. I know I've had several letters come in from watching the committee and from some of the testimony that's come out in previous committee work, so it is an ongoing concern. I'm very thankful that we're moving ahead with our other bill.

We've talked briefly, and we've had questions from the other side of the table and from a colleague on this side as well, regarding the cost of actually moving forward and getting the fingerprints and all that. But what do you think the cost is to Canada and the Canadian taxpayers for the person who has been deported 17 times? What do you think the cost of that would be for the government to have to track these people down, find them, take them through the judicial process and get them out of the country once again? That has to be an enormous cost and burden on Canadian taxpayers as a whole.

Mr. Robert Bell: I would think it's verging on seven figures to get someone out of the country. I don't have numbers, but that would be my impression about every time you have to go through that process.

The other cost is their criminal activity. I don't know what that cost would be, but clearly those are not the actions we want happening in our country.

Ms. Roxanne James: I actually agree with you. First, I have the responsibility to represent my constituents and make sure that their tax dollars are well spent. But to be honest, I'm more concerned about the crime and the criminal factor. If someone's been charged with a serious crime, enough to have the person deported out of Canada, the fact that he or she is able to slip through the cracks and come back again and again and again is even further proof that we need to proceed in this fashion and move forward with biometrics as quickly as possible.

The Chair: Thank you.

Our time has come to an end. I want to thank you, Mr. Bell, Mr. Arnon, and Monsieur Meunier, for taking the time. Your contribution has been very helpful to the committee in our preparation of our report. Thank you for coming.

The next part of the meeting will be in camera, for confidential purposes. The clerk will be asking all those who aren't supposed to be here not to be here.

[*Proceedings continue in camera*]

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

SPEAKER'S PERMISSION

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

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

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

PERMISSION DU PRÉSIDENT

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

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