



House of Commons
CANADA

Standing Committee on Citizenship and Immigration

CIMM • NUMBER 065 • 1st SESSION • 38th PARLIAMENT

EVIDENCE

Tuesday, June 14, 2005

—
Chair

The Honourable Andrew Telegdi

All parliamentary publications are available on the
"Parliamentary Internet Parlementaire" at the following address:

<http://www.parl.gc.ca>

Standing Committee on Citizenship and Immigration

Tuesday, June 14, 2005

•(0905)

[English]

The Chair (Hon. Andrew Telegdi (Kitchener—Waterloo, Lib.)): Good morning. We're going to start our hearings on biometrics.

I would invite any viewing audience we might have to get involved in the debates we have at this committee. We have our parliamentary website, the citizenship and immigration committee website. We'll get a really good sign made up for the future, but it's www.parl.gc.ca/cimm.

There are many studies on the website, and we are very much looking for input from the public. Many of the studies are done by our very able researcher, Mr. Ben Dolin. On the topic we're going to discuss today we have had a previous study done by the previous Parliament, and it is certainly going to be an issue of great debate for anybody.

Other topics that we have covered are also on the website. Just a week ago today we released a report on citizenship revocation, a question of due process and respecting charter rights. It went through the committee overwhelmingly. It's a report that we in the committee believe makes sense. It took the minister less than 24 hours to reject it. The reason for rejection is in the report under "Dissenting Opinion", filed by the parliament secretary.

So I would suggest that viewers look up the report, make up their own minds, and get involved in the process, because ultimately we are here to represent the wishes of the Canadian people, and citizenship is very much an important issue.

Another very important issue is biometrics. Just from personal experience, when I came from Hungary, everybody had to carry an identity card—a passport, if you will—at all times. If you were without the passport, you would be arrested and held in custody until your identity was established.

One of the interesting stories I have, and I think it's worth telling, is that at the time we escaped from Hungary, my parents, mindful of the fact that when we were trying to escape we might get caught, went to the police station and told them they lost their cards, because this gave them an opportunity to get a new set of cards. The thinking was that if they got caught at the border, what would happen is they would take a stamp and stamp your internal passport, and that would alert border people in the future, when you got close to the border, that you were a person to be under a great deal of suspicion.

A lot of debate has gone on in regard to this issue, and I'm sure there is going to be a lot more. Anyway, we're going to ask Mr. Jean

to start off the presentation for the committee on biometric cards, and we'll go to other witnesses as well.

Mr. Jean.

•(0910)

[Translation]

Mr. Daniel Jean (Assistant Deputy Minister, Policy and Program Development, Department of Citizenship and Immigration): Thank you very much, Mr. Chairman.

I would like to thank the Chair and the committee members for accepting our minister's offer to give you a technical briefing session on a field trial of biometrics, an area the department is interested in pursuing. We will be presenting the slides that were sent ahead of time during this morning's technical briefing session.

I'm going to start by introducing my colleagues who are here with me. Ms. Brigitte Diogo is the Acting Director General, Admissibility Branch, where the research and development for this project was done. Mr. Bruce Grundison is the Director of the Biometrics Planning Project. Our important partners are Kin Choi, the Director General at the Canada Border Services Agency, and Randy Jordan, the Associate Director at the CBSA. As you know, the CBSA is our key partner in terms of expertise about intelligence and document integrity.

We will now go to page 2. Mr. Chairman, you mentioned that CIC has been working on issues of document integrity, biometrics and identity since 2001. The former Minister of Citizenship and Immigration referred the policy discussion of biometrics, in the context of discussions about national identity, to the standing committee in 2003. The committee did some work on that at the time.

At the recommendation of the standing committee, as a result of the committee's interim report on the issue, CIC ceased to pursue the issue of national ID further. Since then, the issue has been transferred to the Canada Border Services Agency, as part of the machinery of government process. CIC nevertheless continued to engage in an active policy dialogue on how biometric technology can assist in migration processes. I am here today to inform you of our work to date.

I will turn now to slide 3. I'm here today to give the committee an update on CIC's progress on biometrics in two areas. First, to explain how the exploration of biometrics fits into CIC's long-term planning strategy to improve service and program integrity. Second, I want to explain how biometric technology is an enabler. It will improve facilitation for genuine travellers and promote document integrity, both of which are crucial to the long-term vision of CIC.

We also want to tell you about the planned field trial. Work has accelerated, particularly over the last year. CIC has planned a field trial of biometric technology that will begin in the fall/winter of 2005 and will run for six months. Based on the results of this trial, CIC will develop recommendations for a full program. For the moment, we are talking a field trial.

I turn now to page 4. Before describing the field trial, I would like to outline the context in which this work fits. The US, UK, Australia, European Union and several other countries have pathfinder projects in place. These are projects designed to explore a technology or new business processes. In its turn, Canada is considering testing biometrics in immigration processes.

The testing of biometrics is also an integral part of the border security initiatives being promoted within Canada's national security policy—as you know, this policy was introduced last year, and in particular, the work we are doing with our American neighbour with respect to smart-border management.

Our technology choices will have to meet globally interoperable biometric standards for travel documents (passports, visas and border crossing) being developed through the International Civil Aviation Organization (ICAO). As you know, CIC received funding in fiscal year 2004-2005 for a biometrics planning project.

I turn now to page 5. In order to enhance program integrity, we must have greater certainty of the identity of the person. Clearly, the systems already in place to manage biographical information are important, but CIC needs a tool to help officers match a person quickly to his or her record of status decisions. At a time in which biographical data can be easily copied and fraudulent documents created, documents and text alone are not sufficient.

From the applicant's perspective there are advantages as well, particularly if biometrics are captured as early as possible in the process. That also means that when we try to establish a correlation between an individual and a document, this must be validated and confirmed at each screening point in the usual way, but this is much easier to do using biometrics, once they have been captured. Using biometrics permits a person to identify himself or herself without the need to repeatedly produce documents.

• (0915)

What are the goals of the biometrics field trial?

First of all, the trial will allow us to check the benefits with respect to program integrity and managing identity.

Second, the trial will tell us whether the processing will be faster, with a view to improving client service.

Third, it will tell us to what extent the public accepts biometrics. Polling data indicate that Canadians are relatively in favour of this

idea: 70 per cent of Canadians support biometrics in travel-related initiatives such as border control and passports. However, the programs already in place have not yet touched the majority of travellers. A field trial will also give us some idea about the public's reaction.

In addition, the trial will give us an opportunity to test our regulatory framework and to see its impact on our operations and the adaptations required to ensure—if we go ahead with biometrics in the long term—that this will be done in the most efficient way for our operations.

Finally, it will give us a better idea of the costs involved.

[English]

Turning to page 7, in more detail the field trial will look like this. Two visa officers will collect fingerprints and photo biometrics on a mandatory basis for six months. These will be inkless fingerprints; they will collect the 10 prints. The two designated visa offices are Seattle and Hong Kong, thus one office in Asia and one office in the United States.

Those visa holders will be verified when travelling into British Columbia at Vancouver airport or through the Lower Mainland land border crossing at Douglas. If those same visa clients claim refugee protection in Toronto, they will be identified against the biometric taken at the visa office. We already take fingerprints from refugee claimants, as you know. During that period, we will also be checking the fingerprints of the refugee claimants we receive against the same database to see whether there is any incidence of people coming up in there. If those same clients claim refugee protection in Toronto, they will be identified against the biometric taken at the visa office.

Why these sites? CIC needs to test the use of biometrics across its delivery network of visa offices and in-Canada offices so that it will give us the continuum. We need to know how the process works at CBSA ports of entry. The visa offices in Seattle and Hong Kong have very diverse applicants from all over the world. For a majority of these travellers, the point of arrival is usually British Columbia, and then Etobicoke is our most important centre in terms of the refugee process in Canada.

Going to page 8, we have some numbers. Of course, these are estimates, but we estimate that based on our current trends and historical volumes, we will probably have about 17,300 persons who will participate in the field trial. Of those, 4,800 are people we normally process—refugee claimants—during that same period, who will be checked against the database. The remaining will be people whom we process in the context of our visa offices. These will be temporary residency applicants or applicants for study or work permits who require visas to enter Canada. Only those applying at the field trial visa offices in Seattle and Hong Kong will be scanned for verification. The breakdowns for the port of entry are also indicated.

We estimate there are probably 3,600 persons from that initial population we have defined who will not be verified, for various reasons. It may be that they end up not using their visa at the end; it may be that they receive a visa for a long duration and do not travel during the field trial. There are all kinds of reasons why these people may not be subject to verification during the field trial.

Page 9 gives you an overview of the visa process from application and issuance of visa to arrival at the port of entry. At the two field trial visa offices, applicants who require temporary resident visas to enter Canada will have their fingerprints and facial images enrolled in the stand-alone field trial database. Behind the scenes, the same stand-alone biometric database will be secure in Ottawa, where technical analysis of matches and fraud will take place. At the port of entry, CBSA officers will identify at the primary inspection lane temporary residents who are field trial participants and will request of the participants an inkless fingerprint scan before completing the immigration examination. At the port of entry, only one finger of each hand—two fingers—will be scanned for the verification part of the process.

This overview does not show the refugee process. It's not a new process, as we are already assessing fingerprints of asylum claimants, and it will not appear. There is no change from a client perspective in that particular process.

It should be noted that none of the biometric matching information will be shared with our officers and decision-makers during the trial. It is a trial; we do not plan to use this in enforcing or applying our legislation at this time. This is to prevent erroneous decisions while we are still testing the quality of the information and to protect the privacy of individuals.

For privacy and legal reasons, not all issues can be addressed during the trial in advance of a full biometric program; for example, watchlists and sharing with trusted partners. We are continuing to explore these issues. The trial will not use watchlists, owing to a lack of regulatory authority.

Moving to page 10, protecting applicants' personal information is a top priority for CIC. We will encrypt personal information and store it only in a secure stand-alone database with tightly controlled access. Field trial personnel will sign specific undertakings not to disclose any personal information arising from the trial. After we complete our analysis for the trial, the database will be destroyed. As already mentioned, results from biometric comparisons will not be shared with field officers and will not be used to make decisions about individual clients. This is not the purpose of the trial. Information from the trial will not be shared with third parties

• (0920)

Finally, I'm pleased to advise that CIC's draft privacy impact assessment on the field trial is currently with the Office of the Privacy Commissioner for consultation. It will be finalized following procurement of the technology, and as we've done in other files that involve privacy matters, we will work closely with the Privacy Commissioner.

Moving to page 11, some of the considerations of the field trial, CIC and CBSA are proceeding in partnership to operate the trial at the border sites in Canada as well as in visa offices abroad. Staff

from both departments, who will play key roles in the trial, will be provided with training on the field trial equipment and procedures. Although we expect the trial not to end their regular business, the managers at the participating offices will be able to override procedures if necessary to deal with bottlenecks or unexpected situations. CIC will work with CBSA, its field trial missions, and the Vancouver Airport Authority to ensure that client feedback and concerns are appropriately captured through complaints, procedures, and surveys. As we've said earlier in the presentation, the acceptance by the clients of this new technology for us is very important in our assessment.

Planning has already been under way on the trial for over one year. The estimated cost to run the field trial, including the information technology costs, the temporary field operations personnel, and the communications, is \$3.5 million.

Page 12. We need to take a long-term strategic approach to managing the identity of newcomers to Canada, and we need to phase in our investment to reduce the stress and the cost to the organization. To obtain maximum benefits from biometrics, they should be used throughout the immigration system, from the visa program to arrivals and status programs. A biometric sample collected at our first point of contact with a client will be of value to our program up to the point of citizenship, when other programs such as the e-passport will take over.

As you can see from the diagram, in our trial we'll be testing the first phases of a projected multi-year implementation, and we'll certainly continue to inform the standing committee on the progress in doing this.

Page 13. To wrap up, CIC intends to present our trial concept to stakeholders during the months of June and July. We've already had some informal discussion with stakeholders, and we'll have more formal public sessions and consultations with them. At this point, we anticipate that a request will go out to the vendor community in July for the new technology needed for the trial. The field trial will begin in the fall of 2005 or early winter. Uncertainty regarding timing of the trial is a function of the procurement process that we've just mentioned. Once we have analyzed our findings, the final report and recommendations for implementation of biometrics in CIC will be prepared.

[*Translation*]

Thank you, Mr. Chairman.

I will be pleased to answer your questions.

• (0925)

[*English*]

The Chair: Thank you very much.

Ms. Ablonczy, you were on the trip when you folks went off and you checked these things out in Europe. So it's appropriate you'll be asking the first question.

Mrs. Diane Ablonczy (Calgary—Nose Hill, CPC): Yes. Thank you, Mr. Chairman.

Of course, Mr. Jean is well aware that the committee studied this whole matter of biometrics quite extensively about two years ago. As we're all aware, the recommendation was not to proceed with biometrics for quite a number of reasons. We understand, of course, that with the need to be a little bit more aware of who comes in and out of our country, something has to change. But we want to make sure the change is not just for the sake of change or for optics, that it's actually going to achieve something.

One of the difficulties with biometrics is the unreliability of the use, to some degree. No matter what system you use, there are a number of false positives and false negatives, which makes any identification somewhat suspect. In other words, you may catch somebody who isn't a problem, or think you've caught them, or you may not catch someone who actually is a problem.

I notice with the biometrics now that you're looking at at least two types, fingerprints and facial scans, and that should cut down on the variances. But I wonder if you could give us some idea of exactly what the slippage is in the identification. Have you made that analysis? Have any experts talked to you about that?

Mr. Daniel Jean: Of course, we're working closely with people in the industry, and we are also looking at some countries that are a bit ahead of us in testing this technology, on what the issues are and given reliability.

But to the heart of your question, that's precisely why we suggest going with a trial. We want to go with a trial to be able to test the reliability, to see the impact on our operations. We want to go with a trial where the information is not used in the context of making decisions, primarily to make sure that if there is unreliability or things that have to do with the fact that we're testing an emerging technology, we're not inconveniencing our clients.

We could certainly provide you with some technical information on where some of the biometric technology is in terms of success and reliability and things like that, but I think it would be easier for us to provide you that in writing.

Mrs. Diane Ablonczy: I think that would be helpful, because that's a huge concern.

The other concern, of course, is about privacy. Obviously you're aware of that. I've noted that you'll be talking to the Privacy Commissioner.

To be somewhat candid, government and this department don't have an unblemished record in the area of protecting confidential information or important confidential documents. So there is some real concern there. I think this committee would want to satisfy itself that the holes in the security of the department have been addressed.

Can you talk to us about that and give us some reassurance?

• (0930)

Mr. Daniel Jean: On the issue of privacy, that is paramount to the use of any technology—even more, I would say, when you start using biometrics. However, we should remember that for decades we have been keeping, storing, and maintaining personal information, including pictures of individuals. I think we have a good record of

protecting that information, but we're always looking at ways of improving it, no question about that.

For the purposes of the trial, we've decided to firewall, for normal processes, the information that is going to be collected, stored, and verified. It will allow us to do a trial that gives us a full evaluation of both the benefits and some of the challenges of using such technology. It will also allow us to explore further how we want to go about making sure the privacy considerations are well addressed.

If we were to move forward with implementation in the later round that includes collection and retention of biometrics, we would have to make a regulatory change, and these regulations, of course, would have to extend the utmost attention to the issue of privacy.

Mrs. Diane Ablonczy: I just point out missing computers, break-ins at CIC offices where there is no security, documents going missing....

This is a serious matter. I don't think we can just say, "Well, there hasn't been a problem." There has been. We want to make sure that's not an ongoing concern that we just kind of slough off as parliamentarians.

My last question is with respect to the matter of consultation with other stakeholders, which I understand is taking place in the next few weeks. I wonder if you could give us a list of who will be consulted and whether the committee will be given some kind of summary of the feedback you've had from the stakeholders.

Mr. Daniel Jean: I will make two undertakings. The first is that the consultations are taking place at the end of June, and we will provide you with the list of people who are consulted. I will also try to provide you with a summary of the key issues during these consultations.

I can tell you that we plan to meet with our traditional stakeholders—the Canadian Bar Association immigration chapter and the Canadian Council for Refugees. Some of these groups we've already spoken to informally. We will also invite some other stakeholders who have a key interest in this thing, such as the travel industry and some of our security partners as well.

Mrs. Diane Ablonczy: I would recommend that you also have some heart-to-heart chats with experts in this field. Obviously we could give you some names, but I'm sure you're aware of who the committee has spoken with. These are the ones who will point you to the holes in the system or the vulnerabilities.

The stakeholders, the ones you're mentioning, can only talk in principle, but in the precise viability or feasibility of the technology, you're going to have to consult, really seriously and with an open mind, people who have used the technology or are pretty much aware of how it can work.

Mr. Daniel Jean: Absolutely. This is very important for us. We've already done a number of what we will call literature reviews, in terms of looking at other trials in other countries. We've had exchanges through the multilateral groups we belong to—the ICAO and the IATA working group, in which our partners at CBSA participate—on what the experience of other countries has been. Good information is always welcome.

Mrs. Diane Ablonczy: That's good, because sometimes people conducting the trials want them to work—that's their bias—so it sometimes takes people outside that circle to point out the difficulties. I really want to make sure, if we go ahead with this, that those vulnerabilities are addressed and not just glossed over.

The Chair: Thank you very much.

Certainly, let's remember we're talking about a billion-dollar program. There are a lot of stakeholders who want to make sure it works, because there's a great deal of commercial liability for them.

Next we're going to go on to Madame Faille.

[*Translation*]

Ms. Meili Faille (Vaudreuil-Soulanges, BQ): Thank you.

I would like to thank Diane for her very relevant questions. I think her experience on the committee for many years sheds some light on the issues we are discussing at the moment.

What is the opinion of the privacy commissioner at the moment with respect to the biometrics program? I know that you will be starting discussions on this. In 2003, not so long ago, he did issue a very harsh warning. What has happened since 2003, and what is the commissioner's opinion today?

Mr. Daniel Jean: I do not think I can speak for the commissioner, and it is not my job to do so. However, this is an enabling technology. There is no doubt that the commissioner thinks it is important that in this area, as in any other areas of the same scope, to have rules regarding the collection, retention, manipulation and protection of data. So there must be rules in place to safeguard all these aspects. This is the specific area in which we would like to work closely with the Privacy Commissioner to ensure that these matters are properly managed, both during the trial and during a broader implementation, if we decide to proceed with this program in the future.

• (0935)

Ms. Meili Faille: So you will not deal with that beforehand. Are you making progress with the commissioner at the moment?

Mr. Daniel Jean: At the moment, whenever we intend to implement a new initiative that may have some impact on privacy, there is a privacy impact evaluation done. We therefore gave the Office of the Privacy Commissioner an evaluation that was done by an outside expert and which highlights all the risks to privacy. We explain how we will manage these risks and how we will ensure that we are providing good privacy protection. The next step is for the Office of the Privacy Commissioner to give us its comments.

In the case of initiatives we have implemented in the past, for example the one on frequent travellers at border crossing points which we carried out with Customs Canada—that was before the changes introduced by the machinery of government process—we always considered the comments of the Privacy Commissioner to be very good advice for refining our risk-management strategy.

Finally, we want an initiative that gives us everything we need to improve service, that gives us benefits with respect to document integrity, but also continues to protect our clients' personal information and privacy.

Ms. Meili Faille: Did the commissioner give you an opinion about the pilot project?

Mr. Daniel Jean: The commissioner will be giving us an opinion. We submitted our privacy impact evaluation study, and the commissioner will be giving us an opinion. We always work very closely on this process. There are interactions with the commissioner's office. The office gives us advice on issues and we always consider these suggestions very seriously.

Ms. Meili Faille: I see.

Could you give us some documents, statistics or facts about the falsification of ID documents? I imagine you have done a cost-benefit evaluation and that the project will become cost effective at some point. Is that the case?

Mr. Daniel Jean: Some data already exists on documentary fraud in the financial industry, for example, and also on document integrity. We can indeed see what is available and forward what we find on this matter to the committee.

Furthermore, the reason we are carrying out a test run in the field is because of the cost-benefit analysis. We want to know what sort of benefits we can expect. We don't just want to present biometrics to you from a document integrity point of view. It is also extremely important that we provide you with data as far as the facilitation of services is concerned.

I'm going to give you an example that will require you to be somewhat visionary in your approach. If in 10 years, you end up in a country where, to come to Canada, a visa is required, you may only meet the senior official that is responsible for your file abroad one single time. It's a little bit like when you get your first credit card. A risk assessment is carried out and then you get your first credit card. Your record as a user is what will determine whether or not your card is renewed. In most cases, you never see the people that you dealt with in the beginning.

Currently, we frequently issue long-term visas, in this case five-year visas. We renew them every five years thereafter. This applies to applicants who come from countries where a visa is required. These are legitimate visitors and the department considers them low-risk.

It certainly is possible that such people may one day be authorized to travel without even having to come to our offices. We may no longer need to even see them, as we'd already have their biometric data. We could therefore automatically renew the authorization.

New technologies open the door to a whole host of possibilities capable of facilitating and enhancing customer service. We also want to carry out an assessment in that regard. We don't want to limit ourselves simply to what can be achieved in terms of document integrity.

• (0940)

Ms. Meili Faille: Nevertheless, I would still like to know who is pushing you right now to implement this card project?

Mr. Daniel Jean: First, let me say that there is no card project on the table at the moment. I was simply giving you an example to illustrate how that sort of technology may eventually make the whole process easier. In the long term, we will undoubtedly be able to explore a whole host of avenues.

The fraud that we see perpetrated nowadays is certainly what pushed us down the biometrics path. For centuries, we've used biographical data documents to control people's identity. Then we added a photo. However, with these sorts of documents the nature of the fraud committed is increasingly serious. One example of this is identity fraud. If you look at the options, including photos, biometric data and secured documents issued by competent authorities, clearly biometrics is just one additional way of confirming people's identity.

As we said in our presentation, one of the major inconveniences imposed upon legitimate travellers is the number of checkpoints and the fact that documents are used. Checks have to constantly be carried out to ensure that the person concerned is truly the legitimate document holder. In a new travel environment which would make use of biometrics, we would no longer have to impose such a multitude of inspections on travellers. This holds tremendous potential from a services point of view.

When we look at what is going on in the rest of the world as far as testing such new technology is concerned, one can't help but notice that Canada is somewhat behind. Not by a lot, but given that most countries are a little ahead of us, it would be in our best interest to move ahead right away with this assessment. We need to assess, among other things, what benefits such technology would hold for clients and how it would enhance document integrity. So the objective here would be to define a long-term strategy before actually going ahead and implementing this technology.

[English]

The Chair: Mr. Lui Temelkovski.

Mr. Lui Temelkovski (Oak Ridges—Markham, Lib.): Thank you very much, Mr. Chair.

Thanks to you, Mr. Jean, and your panel as well.

I understand that when people come into the country we issue visas, but we don't issue visas to everybody who comes into the country as a temporary resident, such as those from countries like the United States and countries that are members of the European Union.

Is this pilot project of biometric filing or assessing people, or having them recorded in such a way, to help us manage the number of people who come into the country and leave the country, or is it just a fancy ID card for them?

Mr. Daniel Jean: What we're proposing here today is what we call a field trial. It's to test what the benefits would be in easing travel for legitimate clients and protecting the integrity of our documents, for people applying for visas when they come to Canada and where they're examined at our port of entry. The scope of the field trial does not include people who are from visa-exempt countries. As a matter of fact, the scope from the trial is very limited. It's only for two visa offices, only for people who apply in Hong Kong and Seattle during that finite period of time.

Where are we likely to go in the long term with the use of biometrics in our documents in general? Whether it would be introduced, for example, in our permanent resident card, it's too early to say. We want to assess, first of all, that field trial. We want to see what the advantages are of doing this, both from a client service standpoint and from the standpoint of protecting the integrity of our documents, and then what the best strategy is in the long run. We'll certainly have an opportunity to come back to the committee to update it on our progress.

Mr. Lui Temelkovski: I guess maybe the initial stage is just to gather some data that we may be able to expand on in the future to control entries and exits. Would you agree with that?

• (0945)

Mr. Daniel Jean: That's right. It's not to control entry, I'm sorry, but to see what the benefits of the technology are. In this field trial, or anything we're currently working on, there is no intent to control the entry and exit of people in Canada.

Mr. Lui Temelkovski: So it would not solve our problem of people coming and overstaying?

Mr. Daniel Jean: Well, an entry-exit control would not solve your problem either. There are only a few countries in the world that have what we call entry and exit control systems. Most of them are islands, because these are much easier to operate when you have an island.

If you take, for example, a country such as Australia, what it monitors is overstays. The fact that you know they've overstayed doesn't mean you know where they are, or that you can actually take action against them. Very often, the overstays are also just people who stayed a little longer than they've been allowed to, but they're not necessarily people who, beyond that, are any kind of significant risk to your country.

If you take the example of Australia in the recent past, most of the time the number one source countries of overstays have been countries such as the United States and the U.K.—students going there who have been admitted for six months and decide to stay a couple of months extra for the coral reef or things like that.

An entry and exit system in itself is not an enforcement tool; it's an information tool.

Mr. Lui Temelkovski: Okay. If what you're saying is this will not help us with entry and exit, or knowing how many people have overstayed, then we should be able to tell how many people have overstayed in Canada right now.

Mr. Daniel Jean: We could say that. If we were to try to do an entry-exit control, it would be very difficult also, because we have a land border. The U.K. had an entry-exit control system, which they abandoned when the tunnel was built between France and the U.K. An entry-exit control system, where you're not an island, is a very complex thing.

In the context of the field trial here, what we're trying to do is see.... For years, people have had to have a document to travel; they've had to submit to us some bio data—their name, their date of birth, a lot of very personal information—and their picture. We can even say that in recent years, sometimes when we have doubts about an identity, we're able, because of technology, to exchange pictures over our systems to make sure we're facing the same individual. This is going one step further and saying that by having a biometric identifier, we can be sure the person in front of us is really that person and that the identity or the document has not been tampered with. That's what we're going to test in a very limited scope.

Mr. Lui Temelkovski: One final question. Do we have access to fingerprints from people around the world right now? How many would we have from outside the country? It seems we already have a visa that takes their picture, the application, all the hard facts; the only thing we're adding to this is fingerprints. Unless we have fingerprints of people from all over the world, we're just gathering fingerprints right now. We will initiate....

Mr. Daniel Jean: In the context of the field trial, that's not what we're trying to do. But to answer your question, no, we do not have databases of fingerprints from around the world. But let me take a practical example where, if we were to go in the direction of biometrics in the long term, it could help us.

We have some people we call public safety risks. They are a serious public safety risk, and we remove some of these people two or three times, and they come back and re-enter under a different identity. If we had biometric identifiers, we would be able to know as soon as they arrive at the port of entry that these are people who were removed before. We would know who they are and we would know from our records that they are people who cause a risk to public safety.

That's where, on the public safety front, biometrics in the long run can be a tremendous enabler, in the same fashion that it's going to be a tremendous enabler for the legitimate traveller, who is not going to be inconvenienced at the port of entry, because we know he's a low-risk traveller.

• (0950)

Mr. Lui Temelkovski: Thank you.

The Chair: Now we're moving on to the five-minute round, and we have Mr. Tweed.

Mr. Merv Tweed (Brandon—Souris, CPC): Thank you, Mr. Chair.

Thank you for your presentation. I think what I've heard most when we talk about this type of information collecting and gathering is the protection side and safety.

Who has the most secure system currently operating in the world, as far as this type of information is concerned?

Mr. Daniel Jean: From a privacy standpoint?

Mr. Merv Tweed: Yes. Is there one you would hold above the others, or is there one system you're perhaps tracking and emulating more than another?

Mr. Daniel Jean: Most countries are right now exploring this technology, so it's still early days. In the context of doing our assessment, there is no question that we're going to be trying to look

at best practices in other countries. In looking at best practices, how privacy considerations are addressed will be one of the criteria we'll look at. We're certainly committed to doing that.

Mr. Merv Tweed: Will you be entering into agreements with other countries, not necessarily as far as sharing information but sharing technology is concerned?

Mr. Daniel Jean: Right now we have some agreements. For example, in this specific context, as part of the smart border action plan with the United States, there is a commitment to work towards having interoperable biometrics, so that when people travel they don't have to have.... It's a bit like the early days of your banking card: you had to carry all kinds of different cards, but now they are interoperable. Your bank has your information, and they protect your information, but at least you can....

In the longer run, that certainly is the vision we have around biometrics. Particularly on this continent, because of the importance of movement between Canada and the United States, we have some commitment.

We're a part of some multilateral groups. For example, what we're testing in the context of the field trial are the ICAO standards for facial recognition. The ICAO standards are that you should have facial recognition plus one fingerprint.

We spoke about reliability in some of the questions earlier on. It's one of the reasons we and most countries still use fingerprints: it is the most reliable biometric identifier right now. In terms of a perfect match with no risk, that is one of the most credible ones.

Mr. Merv Tweed: In theory, then, every country is developing its own process, and then it'll be up to someone else or another organization to integrate them. Is that correct?

Mr. Daniel Jean: ICAO is acting very much as a forum for interoperability of these technologies, to make sure the travel industry is not hampered by having all kinds of different things in place.

Mr. Merv Tweed: You mentioned in your report that the field managers will have the authority to override procedures if bottlenecks occur. Are you looking at certain situations, or do you have any idea how or why that might occur?

Mr. Daniel Jean: What we had in mind is, for example, if there is some system dysfunction and it doesn't work properly and it's very slow and we have long lineups at Vancouver airport. It's a field trial, and we do not want the clients to be inconvenienced more than would be acceptable in a situation like that. That's one possibility.

Mr. Merv Tweed: You also mentioned that you'll be looking for feedback from clients and the Canadian public. How do you plan to get those results? Will the Canadian public, other than the people who are being directly affected, even be aware of this?

Mr. Daniel Jean: Because it doesn't involve Canadians as a whole and it doesn't involve permanent residents—it's primarily for foreign travellers—our communication strategy is not one of widely publicizing this trial. It doesn't have an impact on most people.

Certainly, through our strategy of consultations, we are going to talk with most stakeholder groups that have an interest in foreign travellers coming here. People in the context of the trial will be informed of what the trial is all about. In terms of the client satisfaction survey, it'll be people directly involved in the trial itself.

●(0955)

Mr. Merv Tweed: Would it be a fair statement to say that feedback from the Canadian public will be only from those directly involved with the program in the trial implementation?

Mr. Daniel Jean: That would be fair.

Mr. Merv Tweed: Is there a fear that people with an agenda...? How do you ever confirm what information you're collecting from people? If I want to implement something, I'm going to give you the information that allows you to move forward on that path. Is there a check or balance to verify the information, or is it just going to be collected?

Mr. Daniel Jean: Our role is to do public policy, and usually we have to look at all considerations and not just what suits a particular agenda or what suits a particular interest. In doing that, we have to rely on both internal and external resources. For example, when we talk about the privacy consideration, which is probably one of the most critical issues, the Privacy Commissioner and his office come into play and give us that kind of oversight. The work we do with this committee is an important oversight as well, along with the consultations we'll have with stakeholders. We'll be inviting not only stakeholders who necessarily have a stake in travel or have a stake in this technology, or whatever; we'll also have stakeholders who very much have a stake in how our clients are processed and stakeholders who have considerations for privacy. I think that gives you the kind of informed public policy debate that you want to have.

Mr. Merv Tweed: You suggest that the estimated cost of the trial is \$3.5 million. I have a couple of questions around that. Does that include more hirings, or will you be looking at using your current staffing levels? Also, on page 12 you've projected out phase 2, phase 3, and phase 4. Do you have any projections on what those costs may be?

Mr. Daniel Jean: I'll talk about the field trial itself. The field trial itself is managed as a project. For the time being, we have eight people working on the project—designing it, preparing for it, doing the procurement, etc. Once we go into the actual field trial implementation, that team will probably go to 10 people. For the duration of the project we've had to give some temporary resources to our missions in Hong Kong and Seattle and the people who will be involved in that field trial. The summary of the field trial, the field trail itself, is about \$2.45 million; the project management is about \$1 million, for a total of \$3.5 million—and no, we don't have estimates on the future phases, because it will really depend on the evaluation of this field trial.

The Chair: Thank you very much.

Now we're going to move on to Ms. Beaumier.

Ms. Colleen Beaumier (Brampton West, Lib.): Good morning.

I'm new to this, so some of my questions are going to be pretty basic. They're not going to be confrontational either.

Are you saying this program basically is going into effect for identity fraud?

Mr. Daniel Jean: There are two objectives we're trying to test, Madam Beaumier.

One is to try to improve the integrity of our documents—so yes, we're protecting against identity fraud and fraud of documents, because documents are being constantly tampered with. As you know, the fraud industry is a several-billion-dollar industry.

There's also a tremendous facilitation benefit in having this technology. As you probably know, right now in Canada and the United States a number of people have enrolled on a voluntary basis in providing that kind of upfront information for the convenience of not having to be constantly examined when they travel back and forth. At the airport in Vancouver, our colleagues at CBSA are already testing some of that technology in what we call NEXUS Air.

So there are two objectives. One is facilitating legitimate travel; the other is protecting against fraud.

Ms. Colleen Beaumier: We keep talking about protection of privacy. What kind of information from the biometric profile is going to be kept on the database?

Mr. Daniel Jean: This is a field trial, so for the duration of the field trial and the duration of the evaluation that will follow it, we will be maintaining the normal information we have, the bio data. That's your name, your date of birth, where you were born, and these kinds of things, plus an image of yourself, facial recognition. We already do that in our files with a picture, but this time we'll have the actual scanned image and the fingerprints.

This is going to be retained for the duration of the trial and the evaluation. It's going to be firewalled from our normal processes because it's a field trial. We're not using this in our daily operations, and at the end of the project and the evaluation that information will be destroyed, because it's purely for the sake of the study. I guess the best way to describe it is probably to say we're doing a study, but we're doing a field study.

●(1000)

Ms. Colleen Beaumier: What about travel history? There was some talk that airlines were going to be turning over all of their data on their travellers to the CIA. Will your biometric profile contain your travel history over a period of time and your employment? Are we looking at this becoming, instead of just identity fraud protection, perhaps something a little more sinister?

Mr. Daniel Jean: We're already retaining a fair amount of personal information from our clients. We're already retaining an image as well. What we're looking at is whether or not retaining a biometric identifier would help us further in our mission of facilitating the travel of legitimate people and preventing identity fraud. That's purely what we're trying to assess. It's an assessment. In the end it's destroyed. None of that information will be shared with anybody.

Ms. Colleen Beaumier: Let's go to New Delhi just for a moment, my favourite spot. If I go in and apply for a visitor's visa and the visa is not granted, do they do this biometric profiling, this biometric check, before the decision is made, or would they do it after the decision is made?

Mr. Daniel Jean: This field trial is restricted to only two locations, Seattle and Hong Kong, so if you were to go to New Delhi, nothing would happen. But in the context of the field trial, let's say you go to Hong Kong. The biometric is collected at the beginning of the process.

You also need to understand that because it's a study, if people apply by mail, we're not going to collect the biometrics; the biometrics may be collected at the port of entry when someone comes in. Because it's a field study, we don't want to inconvenience our clients.

In the context of people who come in and apply in person, it's going to be collected first. If they get refused, yes, we may have that, but there again, given the scope of the project, this information is not being used for operations. At the end of the study this information is destroyed, as is the rest of the information.

As a matter of fact, if that person were to somehow usurp the identity of somebody else travelling with that identity and were to arrive at the port of entry, the officer at the port of entry would not know that this person was somebody who had applied under a different identity.

Ms. Colleen Beaumier: Yes, but that's under the trial. I think it's fine to look at this and say that at the end of the trial everything is going to be destroyed, but if this program is implemented, nothing will be destroyed after that. I think one of the things we have to look at is beyond the trial.

Mr. Daniel Jean: Of course, once the trial is over, you'll have to do an evaluation of the benefits, the costs, the privacy concerns, and how they can be addressed. Before we move any further on this, we will certainly have a chance to have an exchange with you and with everybody who has an interest in this, presenting how the future of this project may go forward. Right now it's too early to tell.

Ms. Colleen Beaumier: I think one of the dangers, though, in not looking beyond the trial program is...there are plans. If the trial is successful, I can't believe that you're going to begin at that point to decide what's going to be done with this after the trial. I think you already know that.

•(1005)

Mr. Daniel Jean: If the trial is successful—as we hope it's going to be, because let's face it, most countries are moving in that direction—and we decide to go towards implementation and use this in our operations, we will have to adopt regulations, particularly around the privacy considerations. Those are how we collect, how we maintain, how we store, how we protect, and all of these things.

Ms. Colleen Beaumier: Currently regulations aren't reviewed by parliamentary committees. However, I do understand—

Mr. Daniel Jean: Some regulations are reviewed by parliamentary committees.

Ms. Colleen Beaumier: Thank you.

The Chair: Thank you.

Madame Faille.

[Translation]

Ms. Meili Faille: I have a few questions to ask.

You chose two posts with fairly advanced technology. Why did you not chose a post such as Abidjan, Accra or some other similar location? That would have given you a better idea about the feasibility of the project, because the waiting times there are very long. If this technology could be beneficial with respect to documents, it would be particularly helpful in these posts, where errors often happen and documents get lost. There are often crisis situations, and a post is closed down, another is opened elsewhere and the documents are transferred.

Did you consider this option?

Mr. Daniel Jean: We chose these posts in the first place because the numbers of travellers met the requirements for a study of this type. Some of the posts you mentioned did not have a high enough number of travellers.

Second, we did want to limit the scope of the project to the places and border crossing points we were going to be studying. We wanted to isolate missions where we knew that a good percentage of the clients would be entering through the border points that are part of the study. By choosing posts in Asia or Seattle, for the American west, we knew that most of the clients would be entering through Vancouver or Douglas. That was the main reason for our choices.

There is no doubt that when we assess the benefits, challenges and costs of this technology, we will have to know whether it is an enabler for the future. With respect to our client service, we will have to see the impact of this technology in missions where there are problems, such as those you mentioned.

Let us take a long-term example. If a client in Côte d'Ivoire has to go through another country because our office is closed because of problems, and this person is accustomed to travelling in Canada, there will be no problem. In that case, it will be much easier for this individual to get a visa than it is at the moment, because we will already have confirmation of the person's identity.

Ms. Meili Faille: You mentioned that you wanted to study the behaviour of problem cases. Do you have any statistics on this? Are these isolated cases? Some people keep coming back. Have you studied the reasons why people keep coming back after they have been removed from the country?

Mr. Daniel Jean: As I said earlier, we sometimes remove some individuals who belong to more worrisome groups two to four times, because they represent a much more serious risk to the public. These individuals generally come back under a false identity.

When they do return under a false identity—and there are some groups that represent more of a threat—all we have in our files, if we are lucky, is a photograph. It is very difficult for people at our border services to determine that the person is the individual who was removed because he or she committed a crime two years ago.

There is no doubt that this will have a significant impact. Our current data show that there are far more than just a few isolated cases. We have information, although these are not specific statistics, which shows that 5 per cent of cases are people who have been removed more than once. No country has any statistics that are very accurate, and if a country did have such statistics, that would cause me fear.

Ms. Meili Faille: However, the last time we heard that there were problems with the reliability of the technology and risks of errors. Do you have any information about this? What improvements have you made to the project to reduce these technical errors?

• (1010)

Mr. Daniel Jean: First of all, some biometric technology is being used at the moment. In Canada, we have some voluntary programs which use these technologies. We even have one non-voluntary program. There is a technology being tested at the Passport Office. Throughout the world, there are similar projects underway using these technologies. They're much more reliable than formerly.

With respect to biometric identification measures, there is no doubt that fingerprints remain the best way of confirming a person's identity 100 per cent, even though the other technologies are continuing to improve. That is why most countries generally test more than one biometric procedure, but they often go back to fingerprints. It is what is known as the unique identifier, probably the most reliable procedure we have.

The objective of the field test is to determine how reliable these measurements are, but that is not all we want to do. We would not want to set up a technology that results in long delays to our processing times or our procedures at the border. We must be able to incorporate this technology into our operations without causing any major problems for our clients.

Ms. Meili Faille: There are a lot of complaints from people with respect to the Passport Office at the moment. They say that the photographs are too light, or that people are supposed to smile or not, and so on.

How reliable are fingerprints? If they were not taken correctly, do people have to come back and have them taken again? Will the same type of problem exist?

We're talking about two different things. We are talking about fingerprints. In the case of the Passport Office, the issue is photographs.

Mr. Daniel Jean: I'm not a technical expert, so I will not claim to be able to give you the details, but we're talking here about a field test where we will be measuring this type of data and the impact on operations. Obviously, if we were to establish this program in the future, these would be extremely important considerations. However, what we are talking about today is a field test to get more reliable measurements.

The Chair: Mr. Clavet.

Mr. Roger Clavet (Louis-Hébert, BQ): Thank you, Mr. Chairman.

Earlier, I was not here, but the documents state that the biometric information would not be shared. I was wondering whether the obligations made by Canada under the Canada-US agreement excluded such a sharing of security intelligence with the Canada Border Services Agency and with the Canadian Security Intelligence Service.

Can the officials from the department tell us today that this type of biometric information will not be shared by others, or, if such information is shared, under what conditions this would happen?

Mr. Daniel Jean: I want this to be clearly understood by committee members: the information that will not be shared is that collected in the course of the pilot project. We will not use the data we collect during the pilot project.

Clearly, in our routine operations, under our information sharing agreements with the US and other partners, we can share information, including the biometric data we already have. We must remember that in Canada we are already taking the fingerprints of refugee claimants and people with serious immigration problems. If necessary, or by virtue of our information-sharing agreements, we can share this information.

You referred to the agreements with the United States. There is an agreement on information sharing which allows us to give the United States the fingerprints of refugee claimants.

I come back to your initial question. Our commitment is that in the context of this specific project, during which biometric data will be taken from travellers who apply for temporary resident visas in Hong Kong and Seattle, such information will not be shared. It will be used solely for the purposes of the field trial.

[English]

The Chair: Thank you very much, Mr. Jean.

I think the challenge with this always is to make sure that when you reduce dependence on something like biometrics, and you're going to come up with the ultimate smart card, you have to make sure that the system and the integrity of the system is protected, not within the context of a smart card, but I'm thinking about probably the most secure documents we have, which cost the most to produce, the Canadian passport. The security of that, obviously, has been compromised in the past, and no doubt will be compromised in the future.

When we went on the tour for the national ID card, we went across the country and we talked to privacy commissioners. They were all very much against it. Clearly, this is a different kind of situation. I'm wondering if it's going to become a national ID card kind of creed. We tried it with the national ID card, our department was going to get into it, and now we're going this route.

I think the thing to say about this one is it's voluntary for the most part. I suppose if people want to have convenience, they buy into it to that extent voluntarily. The big question that I have, and that a lot of people have—and it's going to be up to this committee to make sure there is scrutiny—is the more we rely on one piece of information, the more we are in trouble if that system is compromised.

I think Mr. Morris Manning made a very eloquent presentation to us in Toronto. You say you're now consulting with people. I would urge you to get hold of Mr. Morris Manning. He filed with the committee—Ben was there—and I think there was a stack of reasons that high of what the problems might be. I'm suggesting that you talk to him, not that he is going to necessarily agree with you, but I think he might raise questions that might help your efforts.

I would like to thank you all very much for appearing. And again I want to remind the viewers that this issue and the national ID card, which was on before, can be found on the parliamentary website for

the citizenship and immigration committee, as well as all sorts of other issues. Thank you very much.

The meeting is adjourned.

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

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

**Also available on the Parliamentary Internet Parlementaire at the following address:
Aussi disponible sur le réseau électronique « Parliamentary Internet Parlementaire » à l'adresse suivante :
<http://www.parl.gc.ca>**

The Speaker of the House hereby grants permission to reproduce this document, in whole or in part, for use in schools and for other purposes such as private study, research, criticism, review or newspaper summary. Any commercial or other use or reproduction of this publication requires the express prior written authorization of the Speaker of the House of Commons.

Le Président de la Chambre des communes accorde, par la présente, l'autorisation de reproduire la totalité ou une partie de ce document à des fins éducatives et à des fins d'étude privée, de recherche, de critique, de compte rendu ou en vue d'en préparer un résumé de journal. Toute reproduction de ce document à des fins commerciales ou autres nécessite l'obtention au préalable d'une autorisation écrite du Président.