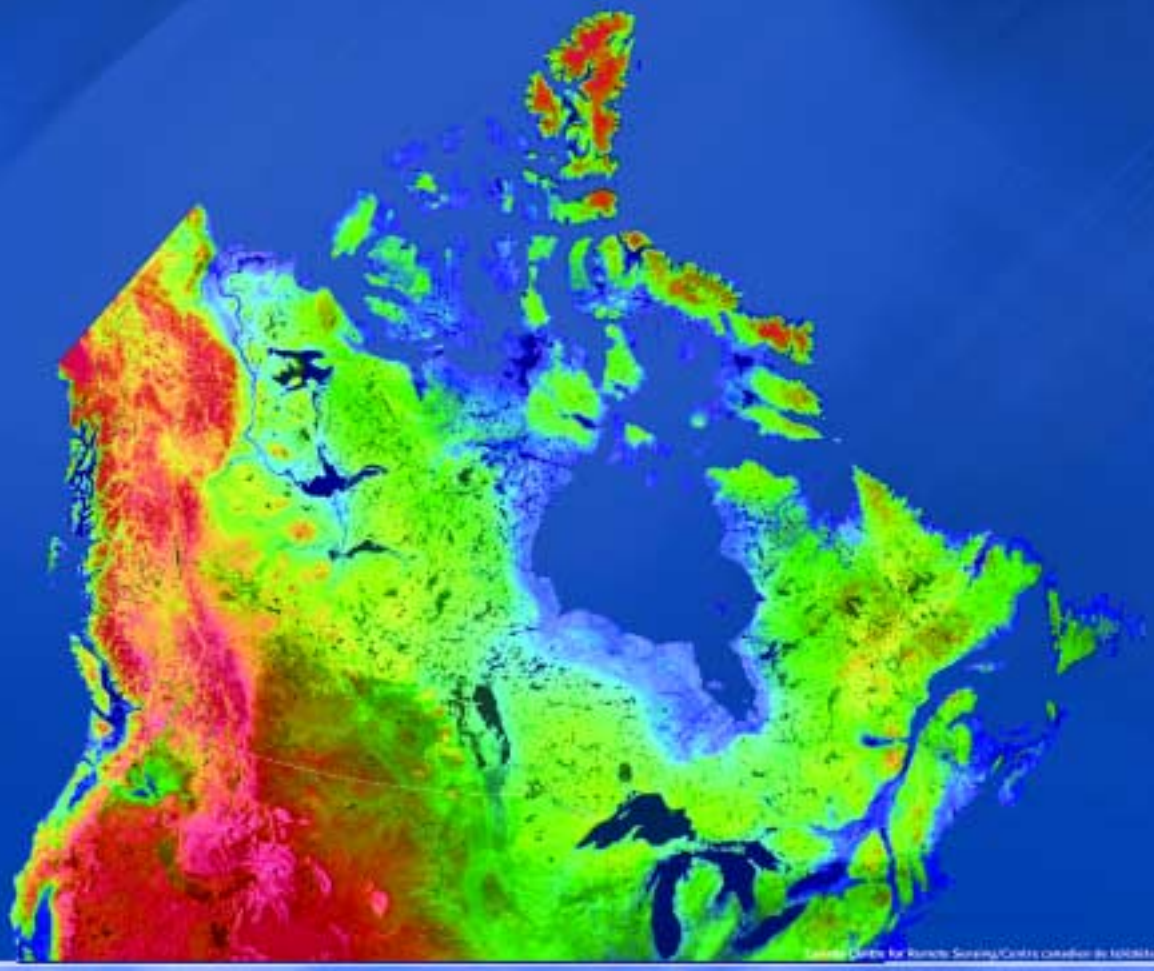
Biometrics:

Implications and Applications for Citizenship and Immigration



Report on a Forum hosted by Citizenship and Immigration Canada

October 7 & 8, 2003 – Ottawa, Ontario

Public Policy Forum
Forum des politiques publiques

Biometrics:

Implications and Applications for Citizenship and Immigration

Report on a Forum hosted by Citizenship and Immigration Canada

October 7 & 8, 2003 – Ottawa, Ontario

Prepared by the Public Policy Forum for:

Citizenship and Immigration Canada

ABOUT THE PUBLIC POLICY FORUM

Striving for Excellence in Government

The Public Policy Forum is an independent, non-profit organisation aimed at improving the quality of government in Canada through better dialogue between the public, privacy and voluntary sectors. The Forum's members, drawn from businesses, federal and provincial governments, the voluntary sector and the labour movement, share a common belief that an efficient and effective public service is a key element in ensuring our quality of life and global competitive position.

Established in 1987, the Public Policy Forum has gained a reputation as a trusted, neutral facilitator, capable of bringing together a wide range of stakeholders in productive dialogue. Its research program provides a neutral base to inform collective decision-making. By promoting more information sharing and greater linkages between governments and other sectors, the Public Policy Forum ensures that Canada's future directions become more dynamic, co-ordinated and responsive to the challenges and opportunities that lie before us.

ABOUT THE AUTHORS

David Brown is Director, Special Projects, at the Public Policy Forum.

David Brook is an Associate of the Public Policy Forum

We would like to acknowledge the assistance of members of the Citizenship and Immigration Canada Task Force on Document Integrity, in particular Peggi McNeil, Director, and of Milena Isakovic, Research Assistant at the Public Policy Forum.

The Public Policy Forum
1405-130 Albert Street
Ottawa, ON K1P 5G4

Tel.: (613) 238-7160
Fax: (613) 238-7990

www.ppforum.ca

TABLE OF CONTENTS

INTRODUCTION

Recent international security concerns, border initiatives and the increasing incidence of identity theft and identity fraud have highlighted the need to strengthen the integrity of Canadian identity, immigration, citizenship and travel documents. Biometric technology has emerged as a powerful and controversial tool that could potentially help to address these public policy challenges. In this context, the Minister of Citizenship and Immigration of Canada, the Honourable Denis Coderre, has encouraged public debate on the issue of the development of a national identity policy and the possible use of biometric technology in identity documentation.

Over the past year, the House of Commons Standing Committee on Citizenship and Immigration has conducted hearings on the merits and challenges related to a possible national identity card. Following extensive consultations, it issued an interim report stating that this issue requires more in-depth study, including engagement with the Canadian public, before any definitive recommendations can be developed. This and related issues are also the subject of federal-provincial-territorial discussions.

On October 7 and 8, 2003, Citizenship and Immigration Canada (CIC), in an effort to advance the public debate, convened a Forum on Biometrics in Ottawa to look at the use of biometrics in the context of measures to enhance the integrity of identity and travel documentation for Canadian citizens and permanent residents (please see Annex II: Agenda).

The objectives of this Forum were to:

- Explore biometrics as a powerful technology that could meet important future policy objectives;
- Enhance and expand the existing discussion on technical and social issues related to the use of biometrics to strengthen document integrity and identity verification;
- Discuss comparative advantages and disadvantages of a comprehensive “national identity card” approach versus a more incremental strategy to improve current, multiple identity documents; and
- Engage in a dialogue on important issues prior to any policy implementation.

Structured around a combination of keynote speakers, panels, and group discussion and feedback, the Forum was designed to raise public awareness and to explore the possible implications and applications of the use of biometric technology in a citizenship and immigration context. The event engaged national stakeholders and international experts from interested sectors in a balanced dialogue to inform and advance the department’s policy thinking on the substantive issues related to the use of biometric technologies to strengthen document integrity (please see Annex III: Registered participants).

In preparation for this event, the Public Policy Forum authored a Background Paper to inform CIC’s policy thinking and to provide Forum participants and the Canadian public with a general overview of the key issues related to biometrics in the context of citizenship and immigration policy[1]. The paper was drafted at the request of CIC, on the basis of research and interviews with key experts (for a brief summary of the Background Paper, please see Annex V).

1 The Background Paper and other documents relating to the Biometrics Forum are available on a Web site created by CIC for the event: **http://cic-forum.ca/english**

In the course of the day-and-a-half session, participants and presenters initiated a dialogue on many of the issues identified in the Background Paper. This report seeks to present the key issues, challenges, directions and questions. It begins with an overview of the key issues that were raised during the Forum and in particular the common themes and points of consensus that emerged. The points made in each of the individual sessions are summarized in Annex I, along with questions and follow-up discussion with participants. In most cases, either the full text or outline notes are available on the Biometrics Forum Web site: **http://cic-forum.ca**.

At the end of the second day, the participants, who were seated at tables of six, were asked to have a "table discussion" on one of three questions relating to the use of biometrics and a possible national identity card. Each table was asked to record its views, and these are summarized in Annex IV. As well, on two occasions during the second day participants were asked to record their views and opinions using an electronic voting tool that allowed for an instant summary of the results. The results of these "instant polls" are summarized in Annex VI.

Forum Proceedings and Conclusions

The Citizenship and Immigration Forum on Biometrics featured a wide range of participants and presenters from many different backgrounds and jurisdictions (please see Annex III for a complete list of participants and presenters). Participants were selected to provide as wide a range as possible of perspectives, positions and opinions on identity, privacy and related issues. Given this diversity of participation, there was a lively debate and dialogue throughout the day and a half of the Forum on many key issues touching on the use of identity documents with biometric features in the citizenship and immigration context.

The Forum began with a keynote dinner address by Professor Alan Dershowitz, Felix Frankfurter Professor of Law at Harvard University (please see Annex I: pp. 8-11), who outlined some of the issues he perceived that relate to a national identity card and the use of biometrics. In his view, there are two key sets of issues: those pertaining to the card itself and those pertaining to its application. Professor Dershowitz emphasized the importance of having the debate about the use of biometrics now, so that policy can drive the development of technology, and not the other way around. He also argued that it is important not to rely on the failure of technology to protect privacy, but rather that issues such as privacy must be addressed at the inception of the development and implementation of any new technology, including an identity card with biometric features.

The morning session began with an introduction by the Honorable Denis Coderre, Minister of Citizenship and Immigration, who outlined the importance of the Forum and the urgency of dealing with issues of identity and the use of biometrics (Annex I: pp. 12-14). He suggested that, although there are a number of important issues to be addressed in relation to the use of biometrics, biometrics as a technology are here to stay. As such, in his view, the status quo is unacceptable and it is important for all Canadians to discuss and debate how best to improve document integrity in order to prevent identity fraud while still protecting the privacy rights of individuals.

The morning session continued with a keynote address by Dr. Colin Soutar, Chief Technology Advisor to the Canadian Advanced Technology Association Biometrics Group, and a leading expert on biometric technologies. He discussed some of the issues concerning the implementation of a biometrics-based identity card, such as the differences between verification and identification (Annex I: pp. 15-18). In his view, it is indeed possible to enhance security while also protecting identity, but this requires identifying the correct policy priorities and building technologies to meet these specifications.

The balance of the morning was spent with a panel of international representatives who discussed the role and application of biometric technologies in their respective contexts (for a complete list of the panelists, please see Annex II: Agenda. Notes on the panel presentation are in Annex I: pp. 19-27.) Panelists discussed the role of biometric systems in immigration in the European Union, through the use of the EURODAC system, and in the United Kingdom. They also examined the importance of biometric technologies to the security agenda in the United States, and the potential use of biometric technologies in the context of immigration and refugee movements to Canada.

During the question period which followed the international panel, participants expressed concern over the potential to create a "we-versus-them" mentality by imposing biometrics in an immigration context. Panelists responded that legitimate users of the immigration system are generally in favour of a single card with a high level of integrity that allows them to access the services they need with a minimum of difficulty. Other Forum participants expressed concern about the potential for abuse of a biometric system. The panelists responded by stating that any system is open to abuse if approached in an inappropriate or irresponsible manner. As such, it is important to ensure an open and transparent debate on the use of biometrics in any given application.

The luncheon speaker was Frank Graves, president of EKOS Research Associates Inc., who presented recent quantitative data on the views of Canadians (Annex I: pp. 28-30). Mr. Graves argued that a clear majority of Canadians would be willing to support the implementation of a national identity card, were they given a compelling reason to do so, but that Canadians do not see the need to trade off security against privacy. He stated that Canadians will demand a high level of both and are not willing to compromise on either.

The afternoon session began with a presentation by Stephanie Perrin of Digital Discretion, who outlined some of the privacy concerns relating to the use of biometrics and the implementation of a national identity card (Annex I: pp. 31-33). Ms. Perrin raised questions about the need for biometric solutions to identity-related issues and stressed the importance of independent oversight of biometric applications and the need for more research into the longer-term implications of the implementation of any national identity card.

The afternoon panel focused on understanding and assessing the privacy implications of biometric technologies in a Canadian context (for a complete list of panelists, please see Annex II: Agenda. Notes on the panel presentation and subsequent discussion are in Annex I: pp. 34-42.) The panelists raised a number of questions regarding the purpose, uses and nature of a national identity card. They also examined the importance of privacy legislation, independent oversight of the use of biometric systems and of data collected through them, and the need to look at alternatives such as improving the integrity of other "root" or "foundation" documents (such as birth certificates). Finally, one of the panelists advanced an argument in favour of a principles-based approach to the use of biometrics.

During the discussion that followed, participants and panelists emphasized the need to ensure the appropriate deployment of biometric technologies, the importance of independent oversight and auditing, and the need for the government to make a compelling case before pursuing the implementation of a national identity card.

The session concluded with participants discussing, at their tables, three issues relating to biometrics, followed by brief reports to the plenary group. The points raised in these deliberations are summarized in Annex IV. Minister Coderre closed the Forum with brief remarks emphasizing once again his belief that biometric technologies are here to stay and that this issue is vital to all Canadians (Annex I: pg. 43). He

expressed his desire to inform Canadians about this issue and to encourage discussions in living rooms across the nation.

Although a consensus did not emerge over the course of the session, nonetheless there were a number of areas of commonality and agreement in support of an agenda to move forward. These key issues, concerns and areas of agreement were:

The use of biometrics in identity documentation presents genuine issues that merit serious public discussion.

- The issues relating to identity documentation have a direct impact on all Canadians. At the same time, public awareness of these issues and of the choices they represent is low and tends to be impressionistic.
- There is currently a policy and legislative vacuum in a rapidly evolving area of public policy.
- Canada has considerable expertise that is relevant to this discussion, both on the technology side and in closely related areas such as privacy and data management. International experience is also relevant, both in providing best practices and because of the interdependent nature of areas of public policy such as immigration.
- There is considerable common ground among knowledgeable experts, recognizing that this is an area that requires a multidisciplinary and multi-jurisdictional approach.

The status quo is not sustainable.

- Canadians cannot rely on the failure or incompetent use of technology to protect their privacy.
- Biometric technologies are now being applied and their use will only grow. It is therefore important to engage in a full and open public debate with respect to their purpose, use, and necessary safeguards against potential abuse.
- It is important to make sure that policy imperatives are driving the development of technology and not technology driving policy.

The perceived dichotomy between security and privacy is false.

- By the end of the Forum, many if not most participants and presenters agreed that although there may be challenges with the use of biometrics in some contexts, there is nothing either inherently privacy-enhancing or privacy-limiting about the use of biometrics. Biometrics must therefore be looked at in the context of specific applications and their related data management environment.

There needs to be a business case for using biometric applications in identity documentation, including a national identity card.

- Participants agreed that there is a real need to define the issues that would be addressed by using biometric tools in identity documentation and the public policy challenges that a single national identity card with biometric features would help to meet.
- These definitions would would make it possible to identify more fully the functions, purposes, uses and safeguards that would be necessary to implement such a card.
- Only when this crucial policy work is completed could a comparison be made between the costs and benefits of a national identity card and other document integrity solutions.

- An important preoccupation for many participants was the cost of establishing a national identity card, including the implementation of an effective process for registration and administrative mechanisms that would be necessary to make it functional on a day-to-day basis. Although there was no agreement on the potential costs of such an endeavour (with estimates ranging from Cdn $340 million to more than Cdn $5 billion), there was general agreement that before such a card can be considered it is absolutely vital to undertake a thorough cost/benefit analysis.

Biometrics have been successfully applied for specific uses in other jurisdictions.

- Presentations throughout the day indicated that biometric identifiers have been successfully used in jurisdictions outside Canada, in the context of addressing clearly identified needs, such as those relating to immigration.
- Some of the lessons from the international examples include:
    - The importance of developing and implementing programs using biometric tools on the basis of sound policy and good management.
    - The importance of understanding the particular application or applications in which biometrics will be used.
    - Privacy safeguards must be built into the system from the outset if they are to be effective.
    - There is a need for effective independent oversight of any technology system that presents a danger of compromising the privacy of any individual or group of individuals.

There are a number of technical issues that would have to be addressed before a biometrics-enabled national identity card could be implemented.

- Participants identified a number of technical challenges and considerations that would need to be considered in the development and implementation of a biometric card, including:
    - Whether the core use of a card is verification or authentication.
    - Ensuring accuracy in the operation of the biometric features and related data management.
    - The method of capturing and processing biometric information (use of an image versus a template).
    - The type of biometric to be used in light of the very different balance of considerations that applies in each case.

A national identity card, if introduced, should be mandatory and not voluntary in nature.

Arguments were presented in favour of both a voluntary and a mandatory approach, however over the course of the Forum the balance favoured making any possible implementation of a national identity card mandatory in nature. Such arguments included:

- The danger of excluding groups who may not be able to access or afford a voluntary card.
- The need to make sure that any infringement on civil liberties is distributed across the entire population, ensuring an open and balanced policy debate.
- At the same time, several participants cautioned against the risk of “function creep” in any national or universal card.

Privacy and data protection issues must be satisfactorily addressed as an integral part of designing and implementing any identity documentation using biometrics.

- Participants expressed concern over a number of potential privacy issues:
    - Unauthorized access to information – participants had a number of concerns around the availability of information that was collected using biometric tools, either to unauthorized government agencies and agents, or to the private sector. A closely related issue is whether and under what terms data would be re-used or shared with others.
    - Function creep – many participants expressed the belief that any card, despite its initial purposes for implementation, will expand in terms of the functions for which it is used. There was particular concern about the extension of a government-issued card's functions into the realms of providing access to government services or even commercial transactions (as is happening in a number of other countries).
    - Privacy principles – at the same time, it was agreed that internationally and nationally accepted privacy and data management principles offer a sound basis to work from in order to regulate the use of biometrics and that useful legislative models exist in Canada.

In the end, participants agreed that there is a need for a "made in Canada" solution to the issue of identity documentation. At the same time, it was recognized that international pressure to implement some form of biometric application, whether restricted to travel documentation or broader in nature, will only increase in the coming years. As such, it would seem that there is a clear and compelling case for the federal government to develop and implement a policy and strategy on identity documentation issues, including the use of biometrics, within its own jurisdiction and to work with the provinces and territories in developing a national approach to these issues. It should also continue to work with international discussion of these issues.

ANNEX I: SUMMARY OF INDIVIDUAL PRESENTATIONS

Opening Event Speech: Balancing Security and Civil Liberties – Prof. Alan Dershowitz
Felix Frankfurter Professor of Law
Harvard Law School

Professor Dershowitz began his speech by deconstructing the issue of the development and implementation of a national identity card into two sets of issues:

- those relating to a national identity card itself, and
- those related to its application in a particular setting.

The first set of issues (those relating to the card itself) are:

1) What type of card to use?

- Would it be a minimal card that might include an individual's name and citizenship, or a maximal card that might include every piece of identifying information about an individual, including their criminal record? Would the card include a biometric identifier?

2) When should government be empowered to require identification?

- When should citizens be able to refuse to identify themselves? It could definitely be argued that the 'feeling of freedom' would be lost if a police officer could ask an individual to produce their papers at any time, for any reason. On the other hand the 'feeling of security' might be compromised if an individual could never be compelled to produce identification.

3) How can you guarantee that the information on a card matches the holder?

- For Professor Dershowitz, this represents two issues: whether an individual presenting a card is the individual represented on the card, and whether the person on the card actually is who they say they are. In his view, the former issue, in particular, lends itself to clarification through the use of a biometric identifier. The latter points to the need for good background checks.

4) Should the card be mandatory or voluntary?

- Professor Dershowitz outlined a number of questions concerning the mandatory versus voluntary implementation of a national identity card. To introduce this discussion, he gave the example of a 'trusted fliers' program that allows one to move through an airport line more quickly if specific criteria are met. The proof of enrollment in such a program could be based on a biometric identifier. Professor Dershowitz asserted that such an application would probably be acceptable to the majority of individuals if the only consequence of non-enrollment was that the non-enrolled individual would be forced to wait in a somewhat longer line. If, however, the enrolled individual moved through the line in minutes, while the non-enrolled individual faced a multi-hour wait, how voluntary is the choice to enroll? Other related questions, in Professor Dershowitz's opinion include:
    - If a card were mandatory, would everyone have to carry it all times?

- If not, would an individual have a grace period within which to produce the card when properly requested to do so?

5) Should an identity card be local, national or international in scope?

- Professor Dershowitz stated that there are advantages and disadvantages to each of these scenarios, but that currently, international standards (such as for driver's licenses) are not widely in use. He mentioned that in the United States efforts have been made to institute a national driver's license, but some conservative as well as civil liberties groups oppose such a plan, with strong opposition even to the institution of a standard-format license across all states.

The second group of issues identified by Professor Dershowitz were those concerning the specific application of a national identity card in a real-world setting, including:

1) What kind of database would be connected to the card?

- For Professor Dershowitz, important questions in this regard include:
  - What information should the database contain?
  - Would it be linked to a single or to multiple databases?
  - Would there be information-sharing between different databases?

2) Should the private sector be able to access this information?

- Professor Dershowitz indicated that there need not be a difficulty in accessing various databases from a single card, as long as the firewall between the databases is sufficiently secure.

3) Is it possible to limit the accessing of information on a national identity card to a 'need to know' basis only?

- Technically, Professor Dershowitz asserted, it is possible to limit access to information. He offered the example of the Malaysian identity card which, as of a few months ago, contained much more information, in his opinion, than any Canadian or American citizen would permit their government to collect in any one place. He indicated that the key to the acceptance of the Malaysian card, however, has been the assurance that no one government agency can access all the information that is contained on the card, as this information is segregated by firewalls and is available on a "need to know" basis only.

Professor Dershowitz continued his address by stating that it is important to have a debate about what kinds of technology are appropriate and in what situations well before the technology is available and on the market, so that policy considerations drive the development of technology and not the other way around. He reinforced this point by stating that one cannot be insensitive to the abuses that can arise from the centralization of power. It is also important to debate what kinds of information are appropriate for governments to gather and hold in databases.

From his general discussion of issues relating to a national identity card, Professor Dershowitz moved to a more in-depth discussion of the ways in which such a card might be implemented. In his view, there are many ways that a national identity card could function – when an individual puts it in a machine, it could give a negative or positive identification, or it could feed out enormous amounts of information from a central database. Either of these functions could be used in any number of applications. He then addressed the concern among some privacy advocates and other participants about the potential for a 'slippery slope,' meaning that the use of ID cards could expand from their primary intended functions to include

other unintended functions that are more invasive of privacy. He stated that the only thing more dangerous than a slippery slope is an 'invisible slippery slope,' recognizing that any card, biometric or otherwise, that offers an improvement on existing methods of verifying identity will undoubtedly begin to be used for unrelated functions. As such, he contended that it is better to have an open and public debate about the possible uses for such a device, rather than letting it be adapted to other functions without debate or scrutiny.

One argument which Professor Dershowitz presented in favor of the implementation of a minimal national identity card was that it could limit the need or rationale for ethnic or national profiling. He argued that if a country is going to diminish rights, it is better for it to spread the diminution of rights across the entire population than to focus it on minority populations (such as American Muslims, following the attacks on September 11, 2001). He stated that if the diminution of freedom is spread across the entire population then there will be a balanced and equitable distribution of any resulting hardship and, as such, there will much more likely be a full and lively debate about its impacts on the population.

Professor Dershowitz then raised the example of the use of face-recognition machines in public places. He argued that although these machines do not currently work well enough to be implemented (they produce far too many false positives and failures to recognize to be effective), they will reach acceptable standards at some point in the near future. He stated that society must start debating the issue of the use of these technologies now, because otherwise it will be too late to initiate a dialogue on these issues when the technology is developed and in place.

One of the central themes of Professor Dershowitz's presentation was the proposition that it is a major error to depend on the inefficiency of technology to protect privacy. He argued that this is a mistake because all technologies, even those which currently seem extremely fallible or remote in their development, will eventually work well enough to be implemented. Therefore, the ideal is to create a "win-win" technology, one that enhances both privacy and security. He stated that policy-makers need to tell the machine-makers what kind of technologies they need to design and create, and that policy-makers need to find ways to increase both security and liberty.

Professor Dershowitz followed his presentation by answering a number of questions from Forum participants. Several participants picked up on his theme of the dangers of function creep (the slippery slope), and expressed concern that this would be an inevitable danger associated with the implementation of any national identification card. In response, he stated that the whole point of having a full and open debate around these issues is to ensure that function creep is not allowed, or at worst, that it occurs after a full and open debate. In his view, doing things in the open is always going to be better than doing things under the table. As such, his final advice to participants was that whatever Canada does in relation to the issue of a national identity card, it should do it openly. He stated that it is important not to count on 'good' coming from the status quo, but to use technology to help solve problems and protect the public good. By the same token, it is important not to reject technology in the belief that good things will flow from inefficiencies.

Opening Remarks – The Honourable Denis Coderre Minister of Citizenship and Immigration Canada

Minister Coderre opened the session by stating that the debate over identity documentation and the use of biometrics is very important to the lives of Canadians[2]. He indicated that, despite differences in perspective among the Forum participants, some issues are universal in scope and must be the subject of a healthy dialogue to allow the country to move ahead. The "biometrics train has left the station," and the issue needs to be discussed with an open mind.

Mr. Coderre identified some of the key issues that Canada must address in the near term, including how to improve document integrity, protect against terrorism and identity theft, and meet emerging international requirements. Document integrity is an issue that all countries face and measures are being taken by the United States, the International Civil Aviation Organization and by the G-8. The question, therefore, is whether we as Canadians want a "made in Canada" solution to these challenges, or one that is imposed from the outside. The planet is getting smaller and documents are increasingly important in the face of the realities of security and terrorism.

A closely related question for the Minister was whether Canada can both protect and enhance privacy while also improving security and ensuring identity. He stated that it seems very clear that this is indeed possible. The entire issue of document integrity is becoming more important since Canadians expect their government to be able to ensure that the people who come to Canada are who they say they are. Canadians also expect the documents they use to access services to be resistant to tampering and fraud and to maintain their integrity over time.

A card is not the full answer to these issues – it fits in a larger set of measures including notably a response to identity theft and identity fraud, which cost Canadians $2.5 billion a year, according to the Canadian Council of Better Business Bureaus. In the United States, the Federal Trade Commission estimates that 10 million Americans were victimized by these crimes in the past year. Statistics show that a thousand people a month report crimes of identity theft to the police, with many more cases unreported. So, while the program cost of a national identity card might be high, the cost of not acting to protect citizens and the economy would be high as well.

Minister Coderre stated that the government understands the need to act. Citizenship and Immigration Canada is in the process of issuing two million new Permanent Resident Cards, a program which has been well received. The use of biometrics is becoming wider spread, and several provinces are considering their introduction, including some that are thinking of using retinal scans and fingerprints on driver's licenses. There is a growing lobby in the United States that wishes to see the implementation of a standardized license with biometric features in every state. Measures are also being taken in the context of airport security. Action on the privacy side is also important, and Minister Coderre flagged the implementation of the new *Personal Information Protection and Electronic Documents Act.*

Minister Coderre stated that the federal government is adopting a more integrated approach to these issues, with Citizenship and Immigration Canada taking a lead on document integrity matters. Doing nothing and hoping for the best is not an option. He outlined two broad possible approaches to improving document integrity:

2 A complete transcript of the Minister's speech is available on the Citizenship and Immigration Biometrics Forum Web site: **http://cic-forum.ca/english**

- A new comprehensive national approach, including looking at options such as a national identity card, or
- An incremental improvement of existing foundation documents.

In either case, in his view, it will be important to look at developing a card (or cards) that make the most of available technologies and that apply best practices. A comprehensive approach might be along the lines of national identity documents adopted by more than 100 countries. The House of Commons Standing Committee on Citizenship and Immigration is already examining these approaches and has studied all aspects of the issue. Fundamentally, the Standing Committee members are asking if a comprehensive approach to the issue of identity is better than an incremental process – can it be used to replace the range of cards now in use by Canadians?

Minister Coderre continued by asserting that, as a country, Canada can also choose to take an incremental approach to improving document integrity that focuses on improving the documents that we already have – and biometrics can be part of this process. He felt it important to note, however, that Canadians already have many kinds of cards that provide information to the government, so it is important not to confuse a desire for anonymity (which Canadians do not currently possess) with the desire to protect an individual's privacy. He suggested that Canadians have already witnessed changes to documents such as their driver's licenses, which are now made of plastic and have photos embedded in their design, and that such changes will only become more commonplace. The names of Canadians appear in many databases and a wide array of individuals and organizations have a considerable store of personal data on many Canadian citizens. In responding to this situation, Canada has two fundamental options: it can maintain the status quo with respect to the privacy of individuals in Canada, or it can look at all the available options to strike a new balance that both enhances security and protects privacy.

In relation to the issue of the identification of landed immigrants in Canada, Minister Coderre stated that the new Permanent Resident card is a better and more secure card than its predecessor document. In his view, however, there is potential to enhance the security of this card through the use of biometric identifiers, which it is capable of incorporating. This leads to some important questions that remain to be addressed:

How do we meet our need for a higher level of security in identity documents?

How do we protect privacy and address concerns about the erosion of our civil liberties?

What would a national identity card cost?

Do we have a cost/benefit analysis that can accurately predict the costs and savings to Canadians?

With respect to the latter point, the Minister suggested that it is important first to agree on concepts and then to discuss costs; the first question that needs to be asked is whether Canadians want a national identity card? This question could be framed by asking what future documentation should look like and how it should be authenticated. In his view, if Canadians were to decide that a national identity card might potentially be a useful tool, then the government should do a cost-benefit analysis and make a business case for its implementation. He stated that the Permanent Resident Card will be issued to approximately two million Canadians and will have an estimated net cost of $22.9 million to implement.

Minister Coderre stated that Canada needs an informed debate on the implementation of a national identity card and that the government needs to put the facts and issues on the table. A decision needs to be made based on sound public policy that will lead to real, tangible improvements for Canadians. Finally,

he asked the rhetorical question, why is Citizenship and Immigration Canada hosting this conference? He responded by stating that, firstly, the department has a duty to explore the implications of any new technologies that could have an impact on its mandate and that would allow it to do its work better. Secondly, Canada needs to look beyond its borders, at other countries such as the United States, the United Kingdom, the European Union, Australia and New Zealand, both to learn from their experience and to look at the impact of what they are doing on Canada.

Canadians have to move beyond thinking about the technical issues involved in implementing a national identity card to thinking about the public policy issues that it would address, and whether these issues present a compelling case for its implementation. The best tools combined with poor policy will simply condemn us to failure, and any use of biometrics as a form of identification and verification must be done in such a way that protects privacy and freedom and that is transparent and open to Canadians in order to ensure accuracy and to prevent abuse.

Canada has a solid basis, however, for developing its policy choices. The *Charter of Rights and Freedoms* and our judicial system give us a base to ensure that we will not become a police state. We can develop a legal framework for the use of biometrics in identity documentation. Biometrics are coming – the Europeans are moving beyond identity cards to smart cards providing access to government services. This is an issue that touches on all aspects of daily life and that requires inclusive solutions.

In concluding, Minister Coderre stated that the discussion in the Forum on Biometrics will be used to develop policy options for the government and to help him as he speaks to his ministerial colleagues and to his international counterparts. This is one of the most important debates of the next decade. The government has a duty to ensure an inclusive, serious debate to allow Canada to adapt to the 21st century.

Keynote Speaker: Biometrics Past, Present and Future – Dr. Colin Soutar Chief Technology Advisor Canadian Advanced Technology Association – Biometrics Group Chief Technology Officer, Bioscrypt Inc.

Dr. Soutar began his presentation by stating that the issue of the use of biometrics in the context of a national identity card is a controversial subject. As such, he made the decision to focus his talk on some of the issues around the use of biometrics in conjunction with the development and implementation of an identity card, and to discuss some of the standardisation efforts that are underway with respect to biometrics both in Canada and internationally.

Within this context, Dr. Soutar indicated that there are a few crucial considerations that must be evaluated in deciding the appropriate implementation of biometrics for a given application. Indeed, he asserted that there are two or three subtle points that are very important to understand in terms of the impact of biometrics on a system as a whole and which have a profound impact on the appropriate deployment of biometric technologies.

As a reference point, Dr. Soutar reviewed some of the current international initiatives with respect to biometric standards. He indicated that the International Standards Organization (ISO) as an organisation is keenly interested in the use of biometrics and that it has a committee, which is currently in the process of defining international biometric standards. He indicated that Canada is a forerunner in the evaluation of security devices and that Canadians (including himself) are helping to define what will, in the future, become international standards.

Dr. Soutar identified four features – fingerprints, iris, hand and face geometry – as being currently the most popular biometric features, from the point of view of international standards development and commercial deployments. He clarified that it is important, especially from the perspective of public perception, that biometrics do not identify a person, but rather that they recognise that someone has been enrolled in a system previously – based on either a search of a database or a one-to-one match. He stated that biometrics could not pick someone out of a crowd, if they have not been previously enrolled, but they can tie a system identifier to an individual.

He asserted that in an appropriately defined system, biometrics could provide additional security and protect confidentiality at the same time. In his view, it is a public policy issue to define the acceptable balance between the protection of civil liberties and the enhancement of security that will be captured within a system. One example he offered of different types of technologies having a differential impact on privacy was the difference between technologies that provide verification and those that identify individuals.

At its most basic, the process of identification uses a database to determine who an individual is, while off-line verification simply demonstrates that an individual matches an identifier on a card. Dr. Soutar stated that it is possible to store information for verification locally (on a card) while identification must take place centrally with the use of a database. In his view, a key challenge with any system of identification is the need for a simple and efficient way to revoke rights and privileges of card holders.

Dr. Soutar argued that the use of biometrics should be complemented with cryptography and smart cards to provide optimal implementation. In other words, technologies need to be combined in order to create an effective system. He also stated that a much broader range of biometrics is currently being deployed than previously and that these technologies are now being combined in novel ways. Some of these novel uses include:

Positive identification – which is useful anywhere where a password or pin is currently used, for example: long distance calling cards, banking, entry to buildings, etc.

Access control – Dr. Soutar used the example of American Express, which uses a smart card with biometrics at their headquarters for purposes of worker verification (to accurately verify who is doing what in the building at what times). This card is local and is used to access buildings across multiple facilities. The New York Police Department also makes use of this technology.

Timekeeping – Another application for biometric cards, which Dr. Soutar described, is time and attendance. He explained that if a number of employees have access to a safe with a biometric system, any individual employee in the presence of the safe at a given time could be accurately identified.

Dr. Soutar concluded this section of his presentation by stating that biometrics are not “coming in the future;” in his view, they are here today.

The next issue, which Dr. Soutar addressed, was the choice of verification versus identification for a biometric system. He indicated that identification can be used for functions such as background checks and involves access to a central database, whereas verification can be used on a daily basis to verify that someone is the valid holder of a card, a process involving only a local data set. As such, he argued, the mathematical matching algorithms for these two operations need not be the same, even though a single acquisition of the biometric can be used for both purposes.

As an example of the uses of verification to protect privacy, Dr. Soutar stated that a user could establish a unique identity via documents such as a birth certificate. A system identifier such as a passport number could be bound to the user's verification template[3] to create a record. In this scenario, the identifier is used only to confirm that the individual who presents the card is who they state they are, and the biometric data is not linked to any other information. Dr. Soutar repeated the point that biometrics themselves do not identify individuals; rather, they recognise that individuals are legitimately enrolled in a system.

Dr. Soutar indicated that a system based on biometric verification would allow for the seamless integration of the new biometric technology with an existing non-biometric system. In this scenario, the 'internal guts' of the database system do not need to know that a biometric is being used to verify the identity of a card holder; the database system is still tied to a separate identifier such as a passport number. Such a system allows the application, not the biometric, to control the rights and privileges of the individual. It also allows the application to easily revoke these rights if necessary.

In Dr. Soutar's view, using an identifier and a verification template also avoids the problem of profiling[4] – all the system needs to know is that a valid passport number is being entered, not who is holding the passport. Once the system has verified the identity of the card holder and shown his or her validity, then the associated passport number is sent to a central application that indicates whether a passport number is valid or not. The implementation of such a system would mean that an officer never has to make the decision about whether someone may validly enter a country; this can be done centrally.

So, can such a system be implemented within Canadian privacy legislation? Dr. Soutar argued that Canada has a good set of privacy standards. Individuals will have expressed their consent when they enrol in a program – they will have an awareness of why the template of their information is being created. He indicated that two privacy principles are of particular importance in this case: the confidentiality of user and of biometric information. In his view, it is important to safeguard the user record by using encryption technology so that the data block cannot be tampered with. He stated that this information can be stored on a bar code and is a very important contributor to the system's integrity.

Dr. Soutar argued that such a system could prevent identity theft and hinder the ability of individuals to use false identities in the commission of terrorist acts. Also, in his view, the separation of user verification from system authorisation limits the danger of function creep.

Dr. Soutar concluded his presentation by discussing the possible uses for biometrics in the future. Some of these uses will involve the fusion of biometrics for convenience and security, such as the combination of face and finger systems and multi-algorithm methods. Another important development, in his opinion, will be the implementation of key binding algorithms, such as templates that are application-specific. A further development might be the use of smart tokens for multiple applications. For example, a key fob could become a multiple key repository, which could access an individual's computer, finances or personal device and would allow the sharing of specific personal information for various purposes.

During the discussion that followed his presentation, a concern was raised that the coding used on cards (for instance the number on a passport) could provide clues as to the identity of the bearer. Dr. Soutar indicated that, in effect, there is no limitation on the identifier, as it does not even have to take the form of a code. He stated that if it makes more sense to have a pseudo-random number assigned as an identifier,

3 A verification template is a unique set of information related to a biometric identifier (such as a fingerprint), which is recorded on a device such as a card, against which a new acquisition of data can be tested.

4 When an agent or officer singles out an individual or group of individuals for particular attention based on an identifier such as race.

then that could be the case. As well, he argued, the number never has to visually appear on the card as it could be encrypted for added security. Finally, he indicated that, from his perspective, any system could potentially be abused, so an analysis of the potential for abuse will have to take place alongside the policy debate surrounding these issues more generally.

Another participant asked whether the use of identification technologies could be used to reduce the incidence of acts of terrorism. Specifically, they asked whether positive identification could stop a rogue officer from doing something untoward, even in an environment that used biometric identification technologies. Dr. Soutar replied by stating that these technologies can enhance security in several different ways: they can act as a deterrent; they can help to prevent identity theft; and, finally, enrolees can be asked to go through a screening process such as that involved in becoming a Canadian citizen – such a screening process can be tied to the ability and capacity to revoke privileges very quickly, if necessary.

Panel Session 1: Biometrics in the International Context

Martin Giles, Assistant Director, United Kingdom Immigration Services, Home Office

Gillian Russell, Directorate General, Justice and Home Affairs, European Commission

Dr. W. Russell Neuman, Senior Policy Advisor, White House Office of Science and Technology Policy

Gerry Van Kessel – Coordinator, Intergovernmental Consultations on Asylum, Refugee and Migration Policies in Europe, North America and Australia

The purpose of the morning panel was to provide an overview of how biometrics are being applied in the international context. The first three panelists were invited to describe the experience in their respective jurisdictions (United Kingdom, European Union and United States), while the fourth panelist was a Canadian working in the intergovernmental environment on immigration and refugee issues.

Martin Giles
Assistant Director
United Kingdom Immigration Services, Home Office

Mr. Giles began his presentation by stating that terrorism is an international problem and requires international cooperation. He continued by describing his involvement with the development and implementation of an immigration biometric identification program in the UK For Mr. Giles, the issue of establishing identity in the immigration process is complex, traditionally relying on passports as a way to identify individuals, provide names, date of birth, nationality and some indication of prior travel. He indicated, however, that this system has begun to break down as many of the individuals who have come to the UK in recent years have destroyed their documents for a variety of reasons.

The very concept of identity itself is interesting, for Mr. Giles, in that most people identify themselves in terms of their names and the area where they live, and yet these things are not unique and thus cannot form the basis of an accurate identification. In his view, biometrics can show the uniqueness of a human being, but only if that individual has not been previously enrolled in the system. The aim of the immigration identity program, therefore, is to ensure that any individual has one, and only one, identity for the purposes of the program.

Mr. Giles stated that in 1999 the UK had a manual system of collecting fingerprints from asylum applicants, a system that was very slow and similar in nature to that in use by Scotland Yard (i.e., by the police). It was taking six months for a fingerprint check to be verified, which was deemed to be an unacceptable length of time. The decision was therefore taken in the late 1990s to re-build the system. As part of their discussions, policy-makers considered whether they should continue to use fingerprints as an identifier or whether they should adopt a new standard. Mr. Giles stated that, for a number of reasons, the decision was made to stay with a fingerprint record: fingerprints are unique, the AFIS (Automated Fingerprint Identification System) is a tried and tested methodology, there are existing records and a statutory right to exchange data with others, in particular the police, and staff were already trained to take fingerprints, which are accepted as evidence.

The original objective of the program to automate the collection of fingerprints from asylum seekers, as outlined by Mr. Giles, was to allow fingerprint tests to be conducted anywhere and to have the results of

these checks available in less than an hour. These parameters were based on the operational experience of the project managers. As a result, currently in each asylum screening unit there are five scanning units and card scanners that can scan in ink fingerprints; these are linked to quick-check units that rely on GSM technology (a second generation wireless technology) and use cell phones to connect to the central system. Mr. Giles stated that the original test project has since been developed into a full program from which biometric cards have been issued that are connected to EURODAC (a European Union-wide database for tracking asylum requests, discussed in the next section of this report). The test project has also led to a similar project with direct links to the police system and the use of this data in visa applications. Finally, Mr. Giles indicated that the system cards have been used to close a loophole that existed in the immigration system whereby individual asylum seekers could change their names and register multiple times in the system.

In Mr. Giles' view, the program has been very successful – multiple applications have been reduced from six to one per cent of the total number of applicants, quick checks are regularly identifying murderers, rapists and other criminals as they access the system, and the application reporting cards are decreasing National Asylum Support Services payments and deterring people from applying for these services by proxy. EURODAC has also identified over 1100 third party applicants, and a recent trial has shown that almost 60 per cent of multiple applicants are being detected by the system.

Mr. Giles stated that there has been vigorous debate around the choice of biometrics for use in this program on an ongoing basis. At the same time, however, in his opinion the benefits are real and tangible. He indicated that some other policy areas where the use of biometrics is being considered include:

- The prevention of the creation of multiple identities,
- Benefit fraud reduction,
- Reporting management,
- Biometric visas,
- Fast-track security clearance,
- Internal security with the Immigration Services (access control and anti-corruption), and
- Biometric passports.

Mr. Giles concluded his presentation by outlining some of the lessons learned from the program. These include:

- Less than 100 per cent accuracy in detection is acceptable as the system can still catch almost 90 per cent of the cases.
- The production of ID cards is difficult when it is dispersed throughout a jurisdiction, but these technical challenges can be overcome.
- Real savings can be realized through the appropriate use of a biometric card system, but biometrics are a new technology and there is considerable ignorance about their use and implications.
- There is a need for international biometrics standards to be able to work in a multi-jurisdictional context. No matter how strong a documentary system, it simply cannot compare with iris and fingerprint-based identifiers.
- Finally, good administration and management are keys to success.

Gillian Russell
Directorate General, Justice and Home Affairs
European Commission

The primary focus of Ms. Russell's presentation was the EURODAC system, which is currently in use in the European Union to keep track of asylum applications in the European Union. Specifically, she focused on some of the issues relating to its successful implementation, and then went on to discuss some new applications for which the EU is considering the use of a biometric database.

Ms. Russell began her presentation by emphasizing the importance of public policy in creating a system such as EURODAC. To this end, she indicated that EURODAC was created as a legal entity only after 10 years of debate about the best way to address the challenge of how to quickly determine if people have applied for asylum in more than one member state. Due to a legal situation, Denmark is excluded, but the system also includes Norway and Iceland (making 16 Member States), and the Swiss are currently negotiating their participation. She stated that EURODAC is the first European-wide biometric database that allows different countries to use their own proprietary information. In fact, each country can use its own system to store fingerprint and other information on the applicant (such as name and sex), but only fingerprint data is transferred to EURODAC for the identification process.

Ms. Russell stated that there are three categories of data in use in EURODAC:

> **Category 1** – asylum seekers over 14, for whom data are stored for 10 years,
>
> **Category 2** – cases of apprehension in an irregular crossing of an external border of the EU, which is stored for 2 years, and
>
> **Category 3** – individuals who are illegally present within a member state, to check for asylum status.

Identification in category 3 could be done with a two finger check, although this is not normal, while other categories require a full 10 prints. Member states are responsible for the gathering and collection of data at one point (national access point), which then sends it to the Central Unit. She indicated that data for the EURODAC system are transferred on the European-wide IPVPN, an Internet-like network that is fully encrypted. Further, she stated that it takes less than five minutes to respond to queries. The system was launched in January 2003 and will expand to include another 10 countries in 2004. It can only be down for 40 minutes per 28 days, which is a very demanding requirement for level of service.

Ms. Russell also gave an overview of some of the different applications in which the EU is considering using similar technologies, such as the system that is used to apply for entry visas to the Schengen group of member states. The common problem to be addressed in this system is that the verification and identification of individuals who have applied for an entry visa in more than one state is an extremely complex task. She indicated that there are some interesting technical challenges to be overcome before such an application could be implemented, with biometrics hopefully providing a useful answer. Indeed, there is a proposal on the table to use biometrics (facial and fingerprints) in new entry visas that would be used solely for identification purposes.

Finally, Ms. Russell discussed some of her concerns about the robustness of some of the new technologies that are currently being proposed, indicating that she is not sure if there has been sufficient research into their effectiveness for very large applications. She stated that there is a strong need for some form of harmonization and that systems will not be able to inter-operate if there is not a common standard in use globally.

In the future, the interchange of data between jurisdictions will depend on standards; this issue is being looked at in many fora including G-8 and other interested international bodies.

To conclude, Ms. Russell stated that in implementing such systems, it is important to be very careful about privacy, an issue which is currently managed by independent bodies in Europe within a legal framework. With EURODAC, the data that is stored belongs to the member state that sends the information. She asserted that these independent bodies can look at how logging is undertaken for the entry and retrieval of data, and how long the logs are kept and provide a means by which anyone can check if their data is stored legally. Within the scope of the other applications the EU is considering, the EU is conducting a considerable amount of research to try to ensure that the technologies that are developed and implemented aid in the development and implementation of good policy to balance the rights of the traveler against various technical and operational objectives, and that there is a coherent approach to the problem of identification.

Dr. W. Russell Neuman
Senior Policy Advisor
White House Office of Science and Technology Policy

The central focus of Dr. Neuman's presentation was technology and border security. He began his presentation by indicating that because of the importance, in their view, of biometrics, the Department of Homeland Security is working on designing biometric research projects to advance their knowledge of its uses and applications in a security context. Further, he indicated that privacy concerns are taken very seriously by the Department, as demonstrated by the presence of a legislatively mandated senior privacy officer who advises the Secretary in charge of these projects.

Dr. Neuman continued by stating that in the White House, the National Science and Technology Council Coordinating Group on Biometrics, in conjunction with over a dozen other departments and agencies, is looking at a series of questions or issues relating to the use of biometrics, including:

- Physical and logical access,
- Biometrics audit and tracking within security systems,
- Immigration,
- Travel, and
- Related applications.

The set of tasks before the coordinating group is to identify gaps in the research and to ensure that these gaps are addressed. As well, the National Institute on Standards and Technology is conducting field accuracy testing of biometrics, while the Technical Support Working Group has funding for industry and is supporting a number of projects relating to the application of biometrics. Dr. Neuman indicated that it is this collection of agencies that is driving the agenda in the United States.

The Coordinating Group has organized the identified priorities into four working groups:

- Biometric modalities (fingerprints, irises, etc),
- Biometric systems and human interface,
- Biometrics fusion, test infrastructure and evaluation, and

- Social, legal and privacy issues.

Dr. Neuman indicated that this last group has been very active and successful. There are, however, in his view, a number of international issues that have not yet been addressed.

In regard to the suggestion that there is a trade-off between privacy and security, Dr. Neuman argued that it is not an either/or proposition. Privacy, in his view, is not synonymous with anonymity, and it is not something that can be derived from the inefficiency of the system. He defined privacy as the ability to exercise personal control over one's identity and how it is used. As such, he expressed the view that privacy is associated with the prevention of identity theft and control over the use of personal information. For Dr. Neuman, protecting privacy means being able to correct an error or prevent fraud associated with a suspected use or misuse of information by authorities. In this context, he provided an example of how a biometric can enhance privacy, such as when an authority looks something up in a system, and their authority to do so is also verified through the use of their own biometric identifier.

Dr. Neuman talked about the need for a "made in Canada" solution and cited, in this context, article 32 of the Manley-Ridge Accord on using joint research. In his view, one of the key issues that remains to be addressed is the use of biometric systems for personal privacy and common security. Article 32 of the Accord emphasizes both of these aspects and draws on what he sees as the inappropriate tension between the two areas of public policy.

Dr. Neuman concluded his presentation by suggesting some potential joint activities between the United States and Canada. He offered as an example follow up to a recent study sponsored by the White House on the accuracy of non-computer aided identification, which might serve as a baseline for future studies. He concluded by stating that the research community currently lacks a benchmark on the number of false accepts and rejects in the human systems of identification that are currently in use.

Gerry Van Kessel
Coordinator, Intergovernmental Consultations on Asylum, Refugee and Migration Policies in Europe, North America and Australia

Mr. Van Kessel is head of an intergovernmental secretariat in Geneva that deals with migration and asylum policies. Previously, he was an official of Citizenship and Immigration Canada. He began his remarks by indicating that he is not an expert on biometrics. As such, the focus of his presentation was on management and policy rather than the technical issues concerning the use of biometrics. He stated that the issue of the use of biometrics is too important to be left to the technologists and that one of the difficulties with technology is that it is an area of mystery and darkness for many managers.

Mr. Van Kessel outlined some current international examples of the use of biometrics. The use of biometrics is greatest at airports through processes called trusted travel facilitation or positive verification. Examples include CANPass at Vancouver International Airport and the INS (Immigration and Naturalization Service) Pass in use in ten U.S. airports. He indicated that there are biometrics applications in place in Singapore, Tel Aviv, Amsterdam, Zurich, Sydney and Sweden. Germany and the Netherlands are piloting biometrics in their visa issuance processes and the United States and the European Union plan to do the same. The United Nations High Commission for Refugees uses a system with Afghan refugees returning to Afghanistan from Pakistan and Italy that has a national identity card that uses biometric identifiers. The International Civil Aviation Organization has set international biometrics standards for travel documents.

In Mr. Van Kessel's view, the question is not whether to adopt biometrics, as it is too late to turn back the tide of biometric technology; rather the issue now is how to manage its applications?

The promise of the use of biometrics in the immigration context, as identified by Mr. Van Kessel, is that they:

- Offer a greater assurance of identity,
- Provide an identification for legal residents and refugees that is universally recognized,
- Facilitate refugee evacuations and repatriations,
- Help to counter fraud and abuses,
- Deter fraud in medical screening and in the case of individuals subject to health checks,
- Reduce the reward for non-compliance,
- Improve the identification of criminals and other risks, and
- Can serve as a unique identifier for improved case processing.

Mr. Van Kessel indicated that the use of biometrics is not simply a matter of realizing potential benefits. He also identified a number of associated challenges. These include:

- Human data entry errors,
- The possibility of malfeasance,
- Quality assurance, and
- The need for frequent training for the administrators of a biometrics-based system.

In his opinion, biometric technologies do not completely solve the problem of identity, as they can be fooled at the point of enrollment. The integrity of a biometric system depends on the quality of the enrollment process.

Mr. Van Kessel indicated that the problem of the protection of privacy requires that safeguards are put in place at the beginning of a system's design, in order to restrict data sharing, function creep and inappropriate data usage. It is his belief that biometrics need not subvert informational privacy. Biometrics can be privacy enhancing if systems are designed with that objective in mind. Another important consideration for Mr. Van Kessel was that all technologies do not have the same level of acceptance by the public, and often there is acceptance of a technology only if it has a perceived benefit. So an important question for Mr. Van Kessel was whether the delivery of a biometric system lives up to its promise of improved security. Does it deliver what it actually says it will? For example, will biometrics really facilitate border crossing?

He continued by talking about the relationship between biometrics and migration and asylum management. There are two categories of individuals who seek to enter countries: those who are allowed to and those who are not. An individual either meets the criteria regarding admissibility or does not. Central to being able to make this determination is confidence on the part of the decision-maker about the identity of the individual seeking to enter or remain in the country. Persons who meet the conditions of entry have no reason not to want to be identified, while persons who are refused entry may seek to create another identity that improves the chances of being allowed to enter or remain. They may be more hesitant to do so, in his opinion, if they know that a biometric identification method will be used to ascertain their identity.

Mr. Van Kessel indicated that there has always been fraud and misrepresentation in immigration, in particular in areas such as family reunification, refugee claims and students who intend to work. The

lengths to which individuals go in hiding their identities is astonishing. So the question emerges, how do you deal with people whose identity and intentions are unknown?

For many, being without documents is the best way to stay in Canada. Mr. Van Kessel indicated that over the past 20 years this has been a growing phenomenon, as have been the efforts of governments to respond to the various aspects of illegal migration, including the problem of documentation and identity. In his opinion, all countries face a challenge in creating documents that respond effectively to the challenge of counterfeiters.

Mr. Van Kessel stated that before September 11, 2001, immigration violations were often viewed as benign. Now, however, this view has changed. Failures in migration management can have serious consequences for public security and identification fraud is a tool of terrorists. So the question is how to identify the people who should be stopped while allowing the rest to travel as they wish? In his view, many elements have to come together to create an approach that works. Biometrics addresses this challenge as it holds out the best chance of identifying individuals and allows for the checking of verified identities against a central database.

Mr. Van Kessel concluded by stating that biometrics will enhance the ability of Citizenship and Immigration Canada officers to make confident and accurate decisions, and will allow for better and faster processing of individuals. When used appropriately, biometrics assist governments in managing the flow of people, however there is a great deal of work still to do before these technologies can be widely implemented.

Questions

Some participants expressed concern about the potential to develop a “we-versus-they” mentality in the implementation of a biometric card and that biometrics would tend to be used to facilitate privileges for the privileged and as a control mechanism for the least privileged. The panelists responded by indicating that, in general, there is support among the lesser privileged for the use of appropriate biometric cards, such as the application of biometrics to registration cards in the UK For some, cards are a way of securing benefits quickly and easily – not only is the process much faster with biometric cards, those with genuine claims usually want some kind of stable document showing their status. At the same time, cards can be used to protect genuine claimants by excluding the people who are not making legitimate claims.

Another point that was raised by a panelist was that there are no clear statistics on the extent of the abuse of the system by refugees, although stories of abuses can be found in every newspaper in the EU In her view, the use of biometric systems such as EURODAC, for instance, may be able to help dispel some of these myths by providing credible and accurate data. Finally, a third panelist indicated that there is a real policy issue in terms of how to balance the rights of refugees versus the right of a country to limit migration. The panelist stated that governments need to address the policy issues first and then move to the technical aspects.

A participant asked for some elaboration on the privacy oversight that takes place on the systems described by the panelists. A panelist responded by indicating that in the EU there is an independent European Data Protection Office, along with a series of independent national data protection offices. These offices conduct audits, and the data protection offices can follow up on transactions and specify how long an immigration office needs to keep archived data. A second panelist indicated that in the UK, there is a legal duty to comply with the *Information Protection Act.*

A final question concerned the potential to use border identification systems as vehicles to identify individuals for harassment or abuse by government. Again, the panel responded by pointing to the

potential for biometric systems to provide the opportunity to introduce objectivity into the process by taking the decision point about identification, or verification of identity, away from a guard or inspection officer and placing it with an impartial vehicle such as the EURODAC system.

One of the panelists summed up the question of the potential for national identity cards to be abused by asking rhetorically, whether there is a history of technologies exacerbating inequality. The answer, in their view, was negative, as biometric technologies give legitimate people easier access to the services they require while reassuring the rest of the public that abuses are being minimized. As to the question of whether technologies can be used for ill, the panelist responded that any technology can be used inappropriately, so it is important to take advantage of the current novelty and interest in biometrics to address fundamental questions of governance and control in order to minimize the potential for future abuse.

Luncheon Speaker – Frank Graves
President
EKOS Research Associates Inc.

The luncheon speech, given by Frank Graves, President, EKOS Research Associates Inc. (EKOS), consisted of a summary and analysis of recent work by EKOS on privacy issues and on the possible implementation of a biometric-enabled national identity card. The findings in the presentation were based on evidence from sixteen focus groups conducted by EKOS in the past year relating to privacy issues. The results are consistent with those from a general survey of 3,000 Canadians.

Mr. Graves' primary contention was that although opponents of a national identity card tend to be more vociferous than proponents, they are not the majority of Canadians. The research undertaken by EKOS indicate that, if the case is made clearly, the public would be open to the inevitability and plausibility of implementing a national identity card.

He continued by stating that while Canadians do have some trouble and concern with the idea of a biometric card, especially around issues of privacy and the competence of governments, these concerns are eclipsed by the clear problems they see with the current system, and other related considerations. In Mr. Graves' view, it is clear that this is not where Canadians were ten years ago. Polls conducted by EKOS in the early 1990s indicated that there was not nearly the same quality or quantity of concern.

Although Canadians feel that privacy is important and that it is under siege, they feel that they are capable of managing these threats. Indeed, concern about privacy has declined over the years and has been displaced by familiarity with new technologies. Citizens have also become less concerned as dire predictions of technological intrusion and catastrophic failures have not come to pass. Mr. Graves noted that although privacy concerns have declined substantially over the past few years, they have gone back up since September 11, 2001. He indicated, however, that although many of the attitudes toward privacy have returned to the levels exhibited prior to this event, security concerns have also remained very high for the Canadian public. At the same time, public confidence in who can take care of privacy issues has shifted away from the private to the public sector. In fact, faith in the public sector, in this regard, is increasing.

Mr. Graves asserted that the Orwellian caveat about the risk of privacy intrusions by "big government" is something that is having a diminishing impact on younger generations of Canadians. For the younger generation, the statement – "I do not mind governments using information if I know about it and can stop it" – elicited agreement from about 75 per cent of respondents. When the same question was asked using

the term “companies” in place of “governments”, the level of support was about 71 per cent in 1992 and has now dropped to about 40 per cent.

Mr. Graves also indicated that Canadians seem to view the perceived dichotomy between privacy and security as being false. They do not see these issues as mutually exclusive and they will demand a high level of both. They are not convinced that bad things are going to happen, however, they also want to see what kinds of safeguards and measures are being put in place.

Another finding that Mr. Graves presented was that since September 11, 2001, many of the population effects that had manifested themselves previously have now dissipated, such as the opposition to immigration from various countries. There does, however, seem to be a permanent backlash against immigration from Arab countries and support for racial profiling. In many areas, such as the economy and feelings towards the state, opinions have returned to pre 9/11 levels, but effects on privacy and security concerns seem to be more permanent in nature.

With regard to Canadian perceptions of risk appraisal, such as the institution of airport taxes and surveillance cameras, they seem to be willing to make specific trade-offs. Consistently, Mr. Graves argued, Canadians seem to line up on the side of security, and yet they do not seem to be so concerned about the issue of terrorism in Canada. He indicated that there is also concern about the Canada-United States relationship, with 50 per cent of Canadians supporting the proposition that there is serious terrorist activity in Canada. Given that the support for a national identity card does not seem to be rooted in a sense that “bad things are going to happen to Canada”, in his opinion, it becomes important to understand where the support for a national identity card is coming from within the Canadian population.

Polls undertaken by EKOS in the past year indicated that about 50 per cent of Canadians believe that the government is a pretty good steward of privacy and that it will not abuse the powers that it is granted, in contrast to 25 per cent who disagree with this statement. Mr. Graves stated that those who are critical, however, tend to be extremely vocal. In both Canada and the United States, there is a plurality of the population who believes that the police should be given more power. If this idea is presented in conjunction with the proposition that Canada needs to do this to fight against terrorism, a clear majority support more police or state power to fight terrorism.

Mr. Graves argued that the concerns about a national identity card seem to be mainly philosophical in nature – that the current generation of Canadians must not compromise the privacy of the next generation to protect their security. There seems to be very strong concern over the potential to compromise the civil liberties of the next generation of Canadians. With that in mind, security does not appear to be the main driver in support of a national identity card; it seems to be as much about the potential for abuse in the current system. Canadians are comparing the advantages of a biometric card against the perception of the kinds of abuses that have taken place with the current system.

Mr. Graves indicated that not only is there majority support for a national identity card, the more respondents learned about biometrics through the EKOS research, and the more they heard about the pros and cons of the card, the more they tended to strengthen their support for a national identity card. Only 6 per cent of Canadians think that the abuse of identity documents is not a serious issue.

A question was asked about the potential for a card to be either voluntary or mandatory in nature. Mr. Graves stated that anything that was voluntary tended to enjoy a higher degree of support than would a mandatory version of the same item, but not by very much. In focus groups, there was more support for a mandatory card because of the feeling that criminals and abusers of the system would not sign up for a voluntary card.

Mr. Graves asserted that when the idea of a biometric feature was presented in conjunction with the idea of a national identity card, it elevated support for the national identity card by a significant degree. For Canadians, the positive aspects of a national identity card are that it can reduce fraud and abuse, provide more accurate identification than that which currently exists, may help with security and might help to maintain access to the United States market. Some of the negative perceptions of the national identity card were in regard to privacy issues, cost, and concern around the potential for a 'slippery slope' effect.

To conclude, Mr. Graves indicated that the government needs a solid rationale for the implementation of a national identity card. Canadians need to understand how it will be implemented, why, what it is going to mean for citizens, and how is it going to work. The public also believes that it is inevitable that this is going to happen so the government might as well plan for it now. There is support among the public for the use of biometrics to reduce fraud and abuse in the system. At the same time there is still a great deal of concern about private sector applications such as the screening of applicants for work (commercial transactions are more of a concern for the public while public uses are less problematic).

In the end, Mr. Graves argued that about 80 per cent of the public think that the implementation of biometric technologies is inevitable. As such, there is strong support for the creation of improved identification documents, with a national identity card being seen as one of many possible vehicles. Currently, pragmatic arguments for such a card seem to trump philosophical arguments against. Few members of the public are actively calling for a biometric national identity card, but there is a general acceptance that such a card may be necessary and that the competence is there within the public service to deal with the privacy issues, should there be a compelling need.

In the discussion, some of the participants expressed concerns about the study and its methodology, citing a methodological slant towards security, the use of biometrics and the impacts of terrorism. They suggested that perhaps technology is not the only solution. Mr. Graves responded to these concerns by agreeing with the caveat about the overuse of technology as a solution. Indeed, he stated that when Canadians were asked how Canada should deal with terrorism in the long term, the top two choices were better forms of intelligence and developing a more multi-cultural and tolerant society.

Afternoon Speaker: Privacy Issues – Stephanie Perrin
President
Digital Discretion Company Inc.

Ms. Perrin began her presentation by stating that she would focus on the privacy issues related to a national identification card, rather than get into the technology. One of her principle points was that there was a rush after September 11, 2001 (9/11) to bring forward technologies that had been 'in the hopper' prior to this event, but for which previously there were no markets. In the wake of 9/11, in her view, such issues as access by law enforcement to personal data, and other aspects of due process have been eroded to the extent that technologies which are extremely damaging to individual privacy could be introduced more broadly and in a number of contexts.

Fundamentally, in the view of Ms. Perrin, there is a need for free speech if democracy is to survive. Although she agreed with Mr. Dershowitz's point from the evening before that relying on the frailty of technology is a fool's course, she stated that there is currently an important debate in civil society over the most appropriate course of action to take on these issues. She stated that the people who criticize the development of a biometric card are not just human rights activists; they are also security and technology experts.

One of Ms. Perrin's major contentions was that rushing to a solution without defining the problem is foolish. Given this contention, she posed the question as to why Canada is rushing to the use of biometrics as a solution. In the border control context, it is a logical step, but in many other instances it may not make sense. Questions need to be asked such as: Are we authenticating individuals? Are we verifying their identity? Are we asking for identity when an anonymous but secure card could serve as well? In her view, there are many ways of dealing with the challenges of identity theft, such as clamping down on easy credit and other steps that privacy advocates have identified. As such, there is no need to implement anything as privacy-invasive as a national identity card.

Canadians, according to Ms. Perrin, have to put the issue of a national identity card in the context of what is happening in the marketplace, given the appetite for transactional data. Ms. Perrin posed the question as to whether the market should be permitted to exercise an uncurbed demand for data. She identified the failure of oversight mechanisms as a primary concern in the implementation of biometric systems. Privacy legislation alone will not protect privacy, she asserted, as the gathering of data causes a problem unto itself and oversight bodies are under-resourced, and they do not have the technical capability to fulfill their roles in protecting citizens in the context of high tech security solutions. She was also concerned that a national identity card will be under-resourced in its implementation; while there are theoretical ways to solve privacy problems they cost money, and the money will likely not be there when the systems are actually built. Furthermore, the cards will be loaded with other applications.

Ms. Perrin suggested that it is dishonest to discuss the issue of a national identity card as anything but a system, existing on a continuum. Canada is embarking on this journey toward a national identity card without first undertaking adequate research. Further, she suggested that the right to privacy is situated in a matrix of associated rights in the Charter of Rights and the Universal Declaration of Human Rights, and other fundamental rights such as freedom of movement and freedom of association are also under threat from a national identity card.

Following this discussion of the relationship of a national identity card to various types of rights, Ms. Perrin looked at the concept of a national identity card from the perspective of ten privacy principles. She stated that accountability is very important, purpose specification is also very important, but that consent is not a realistic expectation in regard to an identity card. She went on to state that voluntary cards tend to become non-voluntary very quickly, which compromises the principle of individual consent. Accuracy is a two-edged sword, as it can be used to compromise individual privacy, which is why sometimes privacy advocates like to see the collection of 'sloppy data', since fewer people can then rely on them for new purposes.

The principle of access was seen by Ms. Perrin to be critical, since an individual has to be able to see and challenge the data that is in these systems if he or she is able to guarantee data integrity. She noted that in Canada an individual does not even have to be the subject of data to challenge its collection and codification in databases under the Personal Information Protection and Electronic Documents Act. This provision specifically addresses the fact that often only the people who are experts in security or systems are able to see what is happening to personal data.

Ms. Perrin stated that there is a fundamental characteristic of biometrics which alarms many people: they pertain to the body. Similarly, biometrics cannot be revoked if they are compromised. Revocation is a key problem and challenge for any authentication system, but especially biometric systems. If the bitstream is compromised, the biometric system will have to permit re-registration of the true individual. One of the big challenges with identity theft right now, she contended, is how does an individual get his own identity back once it is compromised? If a biometric system is compromised, then it is much harder to change the system to re-establish an individual's identity.

Ms. Perrin expressed concern that citizens would be asked for a national identity card as identification in a steadily increasing number of commercial transactions. At the moment, we have an existing problem with the Social Insurance Number, where individuals are asked to produce their SINs at a grocery or Blockbuster video stores. All commercial establishments are looking for secure ID now, and this problem would only be exacerbated through the implementation of a biometric identity card. She stated that in a democracy, there are often citizens who have very little understanding of their rights, and therefore it behooves the government to pay particular attention to ensuring that these rights are not violated.

A further issue that Ms. Perrin identified was the massive costs associated with the implementation of a national identity card. The cost increase would not be arithmetic in nature but rather would increase exponentially with a larger enrollment group. Further, she asserted that the entire concept of oversight is very important and the examples cited of cards in Europe neglect the fact that Europe has an infrastructure of oversight, including the European Court of Human Rights, Universal Data Protection Law, and independent Data Commissioners. We do not have such oversight in Canada. This, in her view, calls into question the ability of the government to implement effective independent oversight of the development and implementation of a national identity card.

For Ms. Perrin, the issues of sovereignty, access to and control of data were also significant. She indicated that for a system to be secure there must be both access and human controls. As an example, she asked the rhetorical question of what would happen if Canadian data are housed in India – is it possible to ensure that the individuals handling Canadian data in India meet Canadian standards of integrity? What rights would foreign governments have to access the data? The answer is simple: all governments have rights to access and collect data from data systems that trump individual privacy rights. Given that very large amounts of sensitive data could be accessed through a national identity card that yields transactional data, choices with respect to technology and data storage and management become extremely important. In her view, the right policies and laws to protect data are necessary but not sufficient; there must be limits to data collection.

Ms. Perrin concluded her presentation by making some suggestions on how to achieve progress in the debate over biometrics. She identified the need to:

- Start a regular dialogue with civil society.
- Find the problems, sketch them out and develop an analytical framework.
- Stop promising a safe world to the public. The premise that giving up privacy can make someone safe from terrorism is a lie. We live in an unsafe world and governments have a responsibility to convey that fact to citizens.
- Provide effective oversight.
- Provide more transparency.
- Do the research.

During the discussion that followed Ms. Perrin's presentation, a participant stated that many Canadians will have biometric cards in the near future and that it is very clear that the rest of the world is moving toward this solution. As such, Canada has some clear options – do nothing or proceed to develop a "made in Canada" solution. Canadians are concerned about function creep and the need for firewalls, but many individuals already use biometric technologies and with knowledge and more information their fears of these technologies subsides.

In response to these assertions, Ms. Perrin indicated that there is a limited ambit in which to carve out a "made in Canada" solution. She stated that one could argue that some groups such as truckers might have a higher acceptance threshold for the use of biometrics than others but that this should not mean that the same standard is applied in every situation. She concluded by stating that the use and collection of data should be appropriate to the situation for which the data are required.

Another participant concluded this portion of the session by stating that there is really a four-part test for the protection of privacy:

- That there is a specialized data protection regime in place,
- Independent oversight,
- The use of privacy impact assessments, and
- The adoption of as many privacy enhancing technologies as possible.

Panel Session 2: Biometrics - Understanding and Assessing the Implications

Dr. Roger Gibbins, President and Chief Executive Officer of the Canada West Foundation

Jennifer Stoddart, Présidente, Commission d'accès à l'information du Québec

Raj Nanavati, International Biometrics Group

Raymonde Folco, Member of Parliament, Laval West

The afternoon panel focused on understanding and assessing the implications of biometrics in the context of a national identity card in Canada.

Roger Gibbins
President and CEO of the Canada West Foundation

Dr. Gibbins began by stating that post 9-11, and in terms of concerns over identity fraud, the use of biometrics seems desirable and useful. As such, his comments addressed two primary topics:

(1) The need for a new national identity card as opposed to the incorporation of biometrics into existing cards, and

(2) Implementation issues

He also indicated that he would focus on the national identity card and not on biometrics more generally. He began by stating that the incorporation of biometrics in a national identity card seems to be less controversial that the implementation of the card itself. For him, the question seems to be - why do we need a third platform for establishing identity? The need does not seem to be intuitive or obvious. An updated passport could be used to travel, so the implementation of an ID card seems to imply the need for biometric identifiers within a domestic context. So what does the government of Canada have in mind? When will Canadians need to produce their card and to whom?

Dr. Gibbins questioned whether the national identification card would be like a passport that could be left at home or like a driver's license that is kept close at hand. He cited the Social Insurance Number as an example of the dangers of function creep, where the Canadian public was assured that it would be used only for a limited purpose while it was soon adopted by the private sector. As such, he stated the belief that any identification card would soon move from public sector applications out into the private sector.

In his view, a new national identification card would soon become a master platform for the public and private sphere, the new gold standard for private and public transactions. He stated that this may indeed become necessary for some transactions. The challenge, in Dr. Gibbins' view, is to make sure that the information is not abused and that the public will not think that it will be used against them at any point. He pointed to the challenge of the Orwellian caveat in terms of the dangers of the misuse of information.

He used the example of the grimness of the new policy that all passport pictures must not feature a smiling individual as an issue that can be dismissed on technical grounds, but not on a political level. Thus, while the introduction of biometrics may be inevitable, in his view the use of a national identity card is not.

Dr. Gibbins also saw the issue of the voluntary versus mandatory nature of the card as being problematic. If the population coverage of a new card were limited, it could become a vehicle for stigmatization and privilege. It could be a badge for the business class or part of the stigmatization of new immigrants. In summary, in his view the card would not be useful unless it was mandatory

Another issue for Dr. Gibbins was the issue of who would pay for the new cards. If it is the users, he thought that the cost would reinforce existing class divisions. He indicated that the overall cost of the implementation of a card was also an issue and that the financial estimates on the costs of implementation should not be believed. He was also concerned that the residents of marginal areas of the country will be outside the coverage of the new card. A final issue he raised was that of the types of information that will be displayed and why on the new cards. Will this information migrate to the private sector? In his perspective, even if the information is protected from function creep into the private sector, the public will still view the card as a link to other functions. The assertion of effective firewalls will not be trusted or believed.

For some, in the opinion of Dr. Gibbins, the implementation of a national identity card will be perceived like the gun registry. He did state, however, that it is not clear how Canadians will react to a biometric card as part of the immigration system. He indicated that there may be more support for the implementation of more extensive documentation on a them-versus-us basis. In many respects, for Dr. Gibbins, the value of the card will hinge its level of integration and inter-operability with the US homeland security provisions. If it is fully integrated, he thought that Canadians would be worried about the flow of information to the U.S., given the current popular resistance to the flow of information to the US. For the implementation of a national identity card to be successful, therefore, he stated that these issues must be solved and addressed up front.

In Dr. Gibbins' view, part of the rationale for a national identity card is fear about new kinds of security threats that may emerge for Canadians in the future. Dr. Gibbins asked, however, whether the need for enhanced security will continue to trump other concerns in the future.

Dr. Gibbins asserted that one way to sell Canadians on the idea of a national identity card is the notion that this card could be the solution to the challenge of carrying multiple cards. If Canadians can use this card to do everything that multiple cards can currently do, then they may be more supportive of its implementation. The development of such a 'super' card, however, would reinforce the deep misgivings that Canadians already have about the surrender of information to the commercial sector.

Dr. Gibbins concluded his presentation by indicating that there may be some real advantages to taking an incremental approach to the implementation of biometrics.

Jennifer Stoddart
Présidente
Commission d'accès à l'information du Québec

Ms. Stoddart began her presentation by indicating that the issue of the use of biometrics in the context of identity verification has been included in a specific law in Quebec for some time: la Loi concernant le cadre juridique des technologies de l'information. Indeed, she stated that historically, in Quebec, particular care has been given to the protection of individual information in general; for example in 1982, the National Assembly adopted the first law concerning the protection of personal information in Quebec. It is during this initiative of the Quebec government that the use of biometrics was first examined. Indeed, following the events of September 11, the enthusiasm concerning biometrics confirmed the choice of the Quebec government to legally regulate their use.

Ms. Stoddart stated that the *Commission d'accès à l'information du Québec* has always expressed reservations about a national identity card. Discussion first arose in Quebec as a result of concerns about potential electoral corruption in some ridings during the 1990 provincial election, and the question was raised as to the feasibility of an identity card for Quebec. The Commission has opposed this and later proposals for a universal identity card and instead has supported a number of other methods of verifying identity that have since been successfully implemented.

La loi concernant le cadre juridique des technologies de l'information du Québec has particular provisions in its legislation that allow the Commission to monitor and control databases of biometric characteristics and measurements. The objective of this legislation is to provide a framework for the use of this information, in particular to provide a measure of protection for electronic transactions, to standardize legal documents and to create a functional equivalence between electronic and paper documentation. In some of these contexts, the issue of authentication becomes a challenge, and Ms. Stoddart recognized that the use of this information on the Internet poses a challenge under Quebec's system of civil law. There are also particular sections in the Quebec legislation that deal specifically with the use of biometrics as a tool for personal identification.

Biometrics are authorized for linking individuals and documents under three conditions:

1. Biometric identification cannot affect the physical integrity of the individual.
2. It cannot be used to link an individual and a location, except for reasons of health and safety.
3. There must be express consent provided by the person concerned and only for purposes of verification and confirmation of identity.

While these provisions have not been tested in court, they are in the context of broader legal protections in Quebec for personal privacy, including that the legal system in Quebec cannot compel anyone to provide a sample of bodily fluid, cannot use a device to find someone, and cannot use a locating device to track an individual.

Ms. Stoddart stated that in Quebec, the use of biometric characteristics for an application would have to pass the test of necessity – requiring a minimum of biometric characteristics – and no recording could be carried out without the knowledge of the individual. The fact that the police lift fingerprints without consent would not serve as a basis for further use of biometric identifiers. Any biometric information that is collected cannot also be used for any other type of decision or purpose, except for verification or confirmation (for example, a drug test could not be conducted on the basis of biometric information collected for an authorized use).

For Ms. Stoddart, another important feature of the Quebec legislation is that information must be disclosed to subjects upon request and biometric identifiers will be destroyed when their purposes have been met. One of the most innovative elements of the legislation is, in her view, the requirement that the existence of all databases of biometric identifiers must be disclosed to the *Commission d'accès à l'information du Québec* – before they become operational and even if they are not in use.

In describing the Commission's powers with respect to databases of biometric identifiers, Ms. Stoddart indicated that they are actually quite limited – it may impose orders on databases with respect to their design and it can suspend a database. The Commission prefers, however, to rely on a self-analysis kit for database administrators and on a privacy impact assessment tool. So far, she stated, there have only been four cases of such databases being developed and implemented in Quebec, most notably: a voluntary database at the University of Montreal athletic centre; a database in a unionized workplace, which raised the issue of the union's ability to provide consent on behalf of its members; and a small biometric database

used in a Hydro Quebec pilot project, which verifies the identity of individuals making large-scale financial transactions.

In conclusion, Ms. Stoddart stated that in Quebec the use of biometrics is seen in the context of privacy rights, which are recognized as a fundamental right and a priority concern for legislators. She argued that for governments that want to implement biometric databases and tools, strict rules should be in place, including that the system must be ultra-secure and its development and use must be compatible with human rights legislation and other privacy principles. Finally, she stated that the Quebec system should be a model for all of Canada and in particular that any initiative must have an expert oversight function from an independent source, such as the *Commission d'Accès à l'information du Québec.*

Raj Nanavati
Partner
International Biometric Group

Mr. Nanavati began his presentation by stating that his firm developed a bio-privacy framework in 1999, in response to requests from clients, and to other indications that there was a need for a privacy framework that specifically addressed issues relating to biometrics. As such, this model ensures that privacy concerns are incorporated at the outset in biometric applications. He indicated that in the past his company has been consulted on the development of the Ontario Health Care Card, which has 12 million users, and by the White House on the Office of Science and Technology Policy on the US Smart initiative, which will involve more than 300 million users. If many individuals are using system such as these, it is vital to adhere to specific privacy and other policy requirements.

The first issue, in his mind, is to define how biometrics relate specifically to privacy concerns. In general, there are two types of privacy – personal privacy and informational privacy. So, should policy-makers consider biometric information to be personal data? In Mr. Nanavati's opinion, since a fingerprint does not provide any information about the individual from which it is taken, a very narrow interpretation could be to conclude that biometrics are not personal data. He indicated that it is often useful, however, to take a broader view of these matters and to look at privacy issues in a wider context.

Mr. Nanavati then discussed the importance of templates. He stated that in particular it is important to know how a template differs from an image. It is extremely important to know what type of image someone is looking at. An image can be related to someone on a one-to-one basis, while a template involves a one-way shift to create a unique signature that is different from the person's image. So, the use of templates, in Mr. Nanavati's view, mitigates some of the concerns about the misuse of data.

Another idea introduced by Mr. Nanavati was that the use of small systems is an important way of protecting privacy. While images are interoperable, templates, for the most part, are not. Since they are not interchangeable, a given technology deployment ties a customer to that one vendor's technology, which limits the ability of outside parties to read or interpret this information. The implications for privacy, in his view, are profound.

One challenge identified by Mr. Nanavati was that biometric data can change over time, so an important issue is how to measure the accuracy of biometric technologies. He indicated that there has been considerable work on scientifically and rigorously evaluating these technologies, given that they are in use by hundreds of millions of individuals. There are three primary errors that can be made by a biometric system: the false match, false non-match, and failure to enroll. He indicated that if a substantial number of people cannot enroll in a system, then it is necessary to have a back-up form of identification and the entire purpose of the system is compromised.

Mr. Nanavati stated that if there is very strict oversight of the enrollment process, then there will be a lower rate of failure to enroll. If, on the other hand, a self-serve kiosk is chosen to enroll the population in a system – a methodology with a high enrollment rate – it could lead to a 10 per cent failure rate. Thus, accuracy rates are based on technologies and specific deployments. He considered that there will always be people who cannot use a particular identifier, for example a small percentage of people do not have a consistent iris and so cannot effectively enroll in an iris scanning technology. So biometrics are not perfect, and there will always be some rate of false match. Mr. Nanavati indicated that the comparison that should be made, therefore, is whether the biometric improves on the existing system's failure rate. For example, in immigration applications, it is important to make sure that biometric failure rates are lower than those for visual matching.

Mr. Nanavati continued by stating that there are four identifiers which are used to evaluate a technology – whether it is privacy invasive, neutral, sympathetic, or protective. Government programs should have 'privacy-sympathetic' as a base-line requirement. In this context, he presented the three primary BioPrivacy functions, as identified by his firm:

- Analysis of biometric applications – impact framework
- Analysis of core technologies – technology risk, and
- Moving toward a privacy sympathetic system – best practices

He asserted that the use of these criteria in evaluating a biometric application ensures an objective framework for evaluation. He used the example of facial recognition technology at the Superbowl as an example of what can go wrong when these technologies are not applied in a consistent manner. At the Superbowl, there were numerous problems with the use of biometric technologies, such as a lack of informed consent on the part of participants – an impact which could potentially have been mitigated by signs that indicated that smart cameras were in use. In Mr. Nanavati's view, it is important to explain to people what is really going on and what the information that is being collected will be used for.

Mr. Nanavati stated that there is considerable confusion about what the term 'biometrics' really means. Some of the focus groups which Mr. Nanavati's organization has been conducting have been enlightening in this regard. In general, people linked fingerprint technologies with the police. After people used a fingerprint system first hand, there was a much higher rate of enrollment, which indicated that they were more likely to accept a biometric identifier once they had first-hand experience with its application. Verification and enrollment can be very simple if done properly. It seems that people need the real-world experience of using biometric applications to really evaluate the feasibility of this technology.

Mr. Nanavati stated that the BioPrivacy framework looks at a number of factors including:

- Optional or mandatory enrollment,
- Overt or covert use of the technology,
- Use for verification or for identification,
- Fixed duration vs. unlimited durations,
- Private sector vs. public sector,
- Individual vs. employee,
- User ownership vs. institutional ownership of data,
- Personal storage vs. template database,

- Behavioural vs. psychological biometric identifiers, and
- Template vs. identifiable data.

He stated that, using combinations of these factors, his firm creates technology risk ratings for various applications.

To conclude, Mr. Nanavati indicated that biometrics could not have done anything, in and of themselves, about the events of September 11, 2001. An identification system in which biometrics are an element could have allowed law enforcement agencies to compare data with criminal or terrorist watch lists. Currently, however, there is not a sizable bank of terrorist signatures or irises, so it is important to consider the use of such technologies closely in an anti-terrorism context.

Raymonde Folco
Member of Parliament, Laval West

Madame Folco began her presentation by differentiating between a principles-based and a more rules-based approach to biometrics. She stated that a rules-based approach lists the social ills to be addressed such as identity fraud, terrorism, and abuse of the system, while a principles-based approach focuses on values. Taking a rules-based approach opens the government to extensive risk. Instead of focusing on statements such as "If we do not break the law, we are within our rights and obligations," Madame Folco posited the view that the government should be looking at the rights of all affected parties. We should be asking, "Which course of action advances the common good, supporting trust, transparency and good governance?"

She went on to identify some of the fundamental architecture that supports the Canadian state such as the *Charter of Rights and Freedoms* and guarantees in the Canadian Constitution. Some of these rights have been curtailed with new security measures. At the same time, new legislation such as the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) and provincial privacy acts also protect citizens' rights to privacy. From this starting point, there are three themes that need to be addressed: security, privacy and human rights, and the relationship among them. In her view, the important question to ask is: what rights do the affected parties have and which approach respects these rights? The more serious the potential for the invasion of these rights, the worse is the course of action.

Madame Folco stated that much of the recent focus in the debate about biometrics has been on security, and that the Biometrics Forum would have taken place even without the events of September 11, 2001. In this world of post-Cold War, open détente and collaboration, Canadians will have to deal with non-state sources of terrorism and identity theft. Economic and social progress is linked to the increased mobility of people, which is linked, in turn, to the ability to prove one's identity. So, she asked, in a new security-conscious environment, what are the new risks and the ongoing risks, and where does this issue of biometrics fit in?

With respect to privacy, Madame Folco asked whether enough was being done to inform Canadians of their choices. Is technology an instrument or a means to an end? Is privacy a value to be protected or a state to be achieved? Thus far, biometrics have been seen as either an unqualified threat or as an enabler of privacy. But, she asked, is the government outlining for Canadians the full scope of each option? Which course of action treats each person the same way, supports fairness and justice, and allows citizens to make their own decisions and to affect their own lives? Does information from polls provide a sound basis for action? What about the silent majority – what representation of the citizenry reflects the actual views of the population? How necessary are polls as a reflection of public opinion? Citizen advocates seem to be

saying 'no' to a national identity card, but how inclusive or exclusive are these groups? Whom do they represent? Ultimately, what is the public willing to compromise in order to get something else? This is an important question in the application of a national identity card. In her view, the facts must be on the table so that citizens can make an informed choice.

The issue of human rights is also important and raises three key issues: Are there differential impacts on different groups (for example, on religious groups)? What kind of society does this encourage? What tools are available to limit differential impacts?

Madame Folco concluded by asking which course of action affects the common good? In her view, the question that must be asked is: Do Canadians have the honesty, courage, compassion, fairness, self control and prudence to confront the real threat of terrorism in Canada without moving to racist generalizations? Does Canada need a new biometric lens in order to assist officials in situations where a purely objective indicator is useful? What is the point of privacy legislation and PIPEDA, and what is the point of a Charter if people cannot feel safe at the same time their privacy is being protected?

So the question remains, does Canada need to incorporate a principles- or a rights-based approach to a national identity card? In Madame Folco's view, any move to adopt biometrics will be an enhancement only if principles and ethics are integral to the approach that is taken and enshrined at each stage of the process. Canada must look at human dignity and worth, assess the product being offered, and examine its benefits versus its costs and its benefits versus its risks. Legislation must protect Canadians. Madame Folco finished her presentation by stating: "Let us control technology instead of technology controlling us."

Questions

Participants began their dialogue with the panelists by asking about the claims that biometric technologies are not yet 'there' in terms of their delivery. One of the panelists responded by stating that this all depends on the need for accuracy – which in turn depends on the deployment. As an example, New York City has been using fingerprint technology to identify welfare recipients for several years. Using facial recognition in airports has not been effective because the technology did not identify terrorists. The technology was deployed in such a way, however, that it was taking photos from 20 feet away with shadows and movement affecting its accuracy. There are some deployments where this technology does not work. You need to look at each deployment on its own and figure out if it makes sense or not.

Another participant suggested that it is necessary to have ongoing independent auditing of some of the intrusive powers that have recently been enacted by government. The panel responded by stating that currently the Treasury Board Secretariat of Canada submits every government project having an impact on privacy to the Privacy Commissioner, and this oversight should be expanded more explicitly in the private sector. Another panelist indicated that parliament responds to what Canadians want, so eventually there will need to be a hard look at the privacy legislation and its impact on issues of verification and authentication.

A final participant asserted that there had been a lot discussion at this session of the use of biometrics for the purposes of matching refugees and asylum seekers. He stated that as a Canadian citizen, he is not coming to the border seeking entry, but is still being told that there is a need for an identity card that can be implemented in a domestic context. He did not feel that the case had been made for such a card. One of the panelists responded by stating that this is a very important point. She indicated that the Biometrics Forum is an initiative of the Minister of Citizenship and Immigration Canada, who has the federal lead on document integrity issues. She concluded that someone had to raise the subject because it had not yet

been discussed. However, in the future, a broader group from across the country, including other levels of government and citizens in general, will have to determine what they want in terms of an identity policy.

Conclusions and Directions for Future Action – The Honourable Denis Coderre Minister of Citizenship and Immigration

The session concluded with remarks by the Honourable Denis Coderre. Minister Coderre began by reiterating his opening remark that this issue is very important both nationally and internationally. He noted that several members of the House of Commons Standing Committee on Citizenship and Immigration had attended the Forum, which he felt had "broken the ice" on a national debate.

Mr. Coderre stated that the use of biometrics is a fundamental issue affecting all Canadians. Citizenship and Immigration Canada has taken a lead in opening up a national debate because it has the lead within the federal government on foundation documents, including citizenship documents and the Permanent Resident documentation (the new Maple Leaf Card). The Minister asserted that biometrics are in use now and they are here to stay. It is not so much a question of "if" but rather of "when." Given the inevitability of this eventuality, Minister Coderre indicated that Canada needs to begin to think about and debate this issue; that the issue of a national identity card needs to be discussed in living rooms across the nation. He indicated that he did not see biometric identifiers as being only for landed immigrants and permanent residents but rather for all Canadians.

In Minister Coderre's view, identity theft, border security, and international standards are all reasons for examining biometrics. It is a Canadian question that requires a balanced approach, but the status quo is not an option. He felt a number of necessary conditions were in place: a strong privacy regime and good institutional working relationships in the privacy field. He liked the Quebec model of providing legislative safeguards for authorized uses of biometrics, because it responds to current realities. As the responsible Minister, he is obliged to cover all the angles and to look at all the possibilities. The national debate has begun and should continue.

Minister Coderre stated that Canada must ensure that its documents are secure without jeopardizing the privacy and values of Canadians. In the next five years Canada will need a million qualified workers and by 2026 demographic growth will be solely on the basis of immigration. He asserted that Canada needs to guarantee the integrity of our foundation documents and protect the identities of our citizens, in order to meet the challenges of this new wave of immigration. At the same time, he recognized that this subject is complex and that the government will have to put in place templates and strategies for firewalls in order to protect privacy while also enhancing security.

In pointing to the evolving nature of the issue, Minister Coderre gave the example of the use of picture identification which, many years ago, was quite controversial. Now, he asked Forum participants to imagine getting on an airplane without a photo ID. He stated that we, as a country, truly have to take a look at the collection of information and the uses of databases. The Biometrics Forum was only the beginning and there will be other steps, but it was a good start. He also looked forward to the final report of the Standing Committee on Citizenship and Immigration. In the final analysis, Canadians will adapt themselves and find a "made in Canada" solution within the global village.

ANNEX II: AGENDA

Tuesday, October 7, 2003 (Fairmont Chateau Laurier Hotel)

TIME	EVENT
5:15	**Registration**
5:30	**RECEPTION**
6:00	**DINNER**
7:20	**Opening Event Speech:** *Balancing Security and Civil Liberties* Professor Alan M. Dershowitz Professor of Law Harvard Law School

Wednesday, October 8, 2003 (National Arts Centre)

7:45	**Registration**
8:20	**Morning Announcements**
8:40	**Opening Remarks** The Honourable Denis Coderre Minister of Citizenship and Immigration
9:00	**Keynote Speaker** Dr. Colin Soutar Chief Technology Advisor Canadian Advanced Technology Association – Biometrics Group Chief Technology Officer Bioscrypt Inc.
9:45	**Instant Survey – Session 1**
10:00	**BREAK**
10:20	**Panel Session 1: Biometrics in the International Context** Martin Giles, Assistant Director United Kingdom Immigration Services Gillian Russell, Directorate General, Justice and Home Affairs European Commission Dr. W. Russell Neuman, Senior Policy Advisor White House Office of Science and Technology Policy Gerry Van Kessel, Coordinator Intergovernmental Consultations on Asylum, Refugee and Migration Policies in Europe, North America and Australia
12:00	**LUNCH**

12:50	**Luncheon Speaker** Frank Graves President EKOS Research Inc.
13:30	**Privacy Issues** Stephanie Perrin President Digital Discretion Company Inc.
2:00	**Panel Session 2: Biometrics – Understanding and Assessing the Implications** Dr. Roger Gibbins President and CEO Canada West Foundation Jennifer Stoddart Présidente Commission d'accès à l'information du Québec Raj Nanavati Partner International Biometric Group Raymonde Folco Member of Parliament, Laval West
3:30	**BREAK**
3:50	**Instant Survey – Session 2**
4:05	**Table Discussion and Dialogue**
4:45	**Where do we go from here? Closing remarks by the Honourable Denis Coderre**
5:00	**End of Forum**

ANNEX III: REGISTERED PARTICIPANTS (AS OF OCTOBER 6, 2003)

Hon. Denis Coderre, P.C., M.P.
Minister of Citizenship and Immigration Canada

Diane Ablonczy
M.P., Calgary-Nose Hill

Reg Alcock
M.P., Winnipeg South

Ken Anderson
Office of the Information and Privacy Commissioner/Ontario

Jahanshah Assadi
UN Commission for Refugees – Canada

Sarkis Assadourian
M.P., Brampton Centre

Rivka Augenfeld
Table de concertation des organismes au service des personnes réfugiées et immigrantes

Bill Bergen
Information Technology Association of Canada

Fariborz Birjandian
Alberta Association of Immigrant Serving Agencies

James Bissett
Public Commentator

Dr. Anu Bose
National Organization of Immigrant and Visible Minority Women

Sam Boutziouvis
Canadian Council of Chief Executives

Robert Bouvier
Teamsters Canada

Brion Brandt
Transport Canada

Patrice Brunet
Quebec Immigration Lawyers Association

John Bryden
M.P., Ancaster-Dundas-Flamborough-Aldershot

Mike Buisson
Royal Canadian Mounted Police

Rose Bullock
Alberta Government Services

Tony Cannavino
Canadian Police Association

Marc-André Charlebois
Association of Canadian Travel Agencies

Anna Chiappa
Canadian Ethnocultural Council

Peter Clark
Standards Council of Canada

Prof. Andrew Clement
Faculty of Information Studies
The University of Toronto

Graham Cooper
Canadian Trucking Alliance

Irwin Cotler
M.P., Mount Royal

Michelle d'Auray
Treasury Board Secretariat

Madeleine Dalphond-Guiral
M.P., Laval-Centre

Raymond D'Aoust
Office of the Privacy Commissioner of Canada

Bob Davidson
International Air Transport Association

Michel d'Avignon
Solicitor General of Canada

Janet Dench
Canadian Council for Refugees

Prof Alan M. Dershowitz
Harvard Law School

Bonnie Diamond
National Organization of Women and Law

Michel Dorais
Citizenship and Immigration Canada

Roland Dorsay
Canadian Airports Council

Ward Elcock
Canadian Security and Intelligence Service

Barry Elliott
Ontario Provincial Police

Warren Everson
Air Transport Association of Canada

Dr. David Flaherty
Privacy and Information Policy Consultant

Jean-Guy Fleury
Immigration and Refugee Board of Canada

Raymonde Folco
M.P., Laval West

Joe Fontana
M.P., London North Centre

Bridget Foster
Atlantic Regional Association of Immigrant Serving Agencies

Dr. Roger Gibbins
Canada West Foundation

Martin Giles
UK Immigration Services

Frank Graves
EKOS Research Associates Inc.

Roy Gray
Indian and Northern Affairs Canada

Art Hanger
M.P., Calgary Northeast

Jonathan Hatwell
Delegation of the European Commission in Canada

Ryan Higgitt
Student

Peter Hope-Tindall
data Privacy Partners Ltd.

Martin Huddart
International Biometric Industry Association

Thelma Johnson
Vital Statistics Council of Canada

Catherine Johnston
Advanced Card Technology Association of Canada

Onno Kremers
Human Resource Development Canada

François Laporte
Teamsters Canada

John Lawford
Public Interest Advocacy Centre

Anne Legars
Shipping Federation of Canada

Sophia Leung
M.P., Vancouver-Kingsway

Alfred MacLeod
Citizenship and Immigration Canada

Inky Mark
M.P., Dauphin-Swan River

Robert Marleau
Office of the Privacy Commissioner of Canada

Robert Martel
Inuit Tapiriit Kanatami

Gordon Maynard
Canadian Bar Association

Kathryn McCallion
Department of Foreign Affairs and International Trade

Steve McCammon
Canadian Civil Liberties Association

Gary McDonald
Department of Foreign Affairs and International Trade

Kevin McGarr
Canadian Air Transport Security Association

Paul McGrath
Canadian Bankers Association

Michael N. Murphy
Canadian Chamber of Commerce

Raj Nanavati
International Biometrics Group, LLC

Dr. W. Russell Neuman
The White House

Massimo Pacetti
M.P., St Léonard-St Michel

David Paterson
CATA Alliance

Chantal Péan
Canadian Tourism Association

Bill Pentney
Citizenship and Immigration Canada

Stephanie Perrin
Digital Discretion Company Inc.

Thao Pham
Privy Council Office

Jim Phillips
CAN/AM Border Trade Alliance

Jerry Pickard
M.P., Chatham-Kent-Essex

David Price
M.P., Compton-Stanstead

Yves Prud'Homme
Fédération des policiers et policières municipaux du Québec

James Puleo
International Organization for Migration

Hon. Robert K. Rae, P.C., O.C., Q.C.
Goodmans LLP

Raj Rasalingam
Pearson-Shoyama Institute

Glenn Robinson
Privy Council Office

Gillian Russell
European Commission

Gerry Salembier
Finance Canada

Ravi Sall
Citizenship and Immigration Canada (Youth Network)

Dr. Marc Saner
Institute on Governance

Dr. Colin Soutar
Bioscrypt Inc./CATA Alliance

Johanne St-Cyr
Canadian Council of Motor Transport Administrators

Valerie Steeves
Carleton University

Jennifer Stoddart
Commission d'accès à l'information du Québec

Tamy Superle
Student

Roch Tassé
International Civil Liberties Monitoring Group

Maureen Tracy
Canada Customs and Revenue Agency

Gerry Van Kessel
Intergovernmental Consultations on Asylum, Refugee and Migration Policies

Sandi Villeneuve
Association of International Customs and Border Agencies

Diane Vincent
Citizenship and Immigration Canada

Venita Warren
Citizenship and Immigration Canada (Youth Network)

Robert Whitelaw
Canadian Council of Better Business Bureaus

Randy Williams
Tourism Industry Association of Canada

Patricia Woroch
Immigration Services Society

Lynne Yelich
M.P., Blackstrap

Dr. Elia Zureik
Queen's University

ANNEX IV: TABLE DISCUSSION AND DIALOGUE

At the conclusion of the session, participants were given approximately forty-five minutes to discuss several key issues at their tables. This section seeks to capture both the oral reports to the plenary session at the end of the table discussions and the comments recorded in work books at each of the tables.

Issue 1*: It is generally agreed that privacy is a fundamental concern when considering changes to improve the integrity of our documents. If biometric features were adopted as part of measures to improve document integrity,*

- ***What kinds of safeguards need to be put in place to ensure adequate privacy protection?***
- ***Do existing privacy safeguards (legislation, policy, institutions) provide a sufficient basis for dealing with the introduction of biometric identifiers?***
- ***What role does technology play in ensuring appropriate checks and balances?***

In response to the first question, the safeguards that participants identified included:

- The limitation of scope creep,
- Appropriate protection of biometric data,
- An independent oversight function based on statute, and
- Clarity and transparency around the systems purposes and processes.

On the question of existing privacy safeguards they felt that:

- Currently, there are not enough safeguards to prevent unauthorized use by the private sectors.
- There needs to be a better accountability framework.

Finally, participants felt that technology could play many roles. It could provide:

- Audit capability, and
- Counterfeit and tamper resistance that is appropriate to particular functions.

Issue 2: *Document with biometric features can be implemented in programs with either voluntary or mandatory enrollment. If the goal of document integrity is to produce better, more secure documents that are less susceptible to counterfeiting and ID theft, many suggest that mandatory enrollment is required. On the other hand, privacy concerns suggest that individuals need to have a choice of whether or not their biometric is on a documnt or in a database. What do you think?*

Participants felt that there are important privacy implications to a national identity card whether or not it is mandatory. They felt that a business case should be made for the implementation of a national identity card, based on cost-benefit comparison versus document integrity solutions. There also has to be more discussion of the fundamental purpose of the card.

Some participants felt that this question was premature given that the government has not decided what the card will be used for. There was also concern about the eventual contracting out of card functions and the potential challenges this would create. Finally, there was concern that the uses for a national identity card would creep into unintended areas.

Issue 3: *In the current international security and law enforcement environment there is concern about document integrity in the context of travel and international movement of people. A number of jurisdictions (including most of Canada's major trading partners – USAs, EU, etc.) and international organizations are taking steps to introduce biometric features into travel documentation over the next two or three years:*

- ***What should Canada's response be to these developments?***
- ***How much scope does Canada have to act independently in this sphere?***

Some participants asked why we are leaping to the use of biometrics as a solution to a question that is not well understood. They asked whether Canada has ruled out other approaches such as the development of secure credentials in place of a national identity card. Others saw the need to develop such a card, in order to keep pace with our major trading partners. Initiatives that they suggested could be explored included: looking at travel documents, participating in standards bodies, and other activities to ensure that we are shaping the outcomes of international discussions on standards and priorities in a way that is acceptable to the collective values of Canadians. They stated that if Canada is to pursue such initiatives, then Canada should find like-minded partners with whom to work on developing effective international standards.

Other participants stated that there are a number of issues relating to the implementation of a national identity card that were not addressed at the Forum, including:

- The system of registration,
- Trade implications, both good and bad,
- Access to other landmasses besides North America,
- Sovereignty,
- Ethics and dignity,
- Revocation, and
- Is there a plan B for "when stuff happens," i.e., a worst case scenario?

ANNEX V: SUMMARY OF PUBLIC POLICY FORUM BACKGROUND PAPER

At the request of Citizenship and Immigration Canada, the Public Policy Forum prepared a background paper for the Biometrics Forum. This annex provides an overview of the paper. The full text of the the Background Paper and other documents relating to the Biometrics Forum are available on a Web site created by CIC for the event: **http://cic-forum.ca/english**.

Some of the key considerations with respect to the possible use of biometrics that were discussed in the paper included:

1) Applications

- *Identification versus verification*

2) Types of biometrics

- *Physiological characteristics versus behavioural characteristics*

3) Uses, including:

- *Storage on a computer chip*
- *Encryption on national identity cards*
- *Use in citizenship, immigration and travel contexts*

4) Performance Measurement

- *False rejection rate*
- *False acceptance rate*

The Background Paper also suggested a number of key questions for consideration in a public policy context:

1) Balancing security, privacy and civil liberties

- *What are the public values that should underpin decisions about the use of biometrics in citizenship and immigration identity documentation?*
- *Is the relationship among these values a zero-sum game? For example, is an increase in privacy protection necessarily at the expense of security (or vice-versa)?*

2) Purpose and Application

- *What public policy objectives will be served through the use of biometrics technologies in citizenship and immigration documentation?*
- *What applications (identification vs. verification) would be used?*

3) Privacy-enhancing technology and information management

- *Are technologies available that will ensure adequate protection of privacy and protection of personal information?*
- *What government databases would be linked to biometrics-enabled documentation? How would information be managed?*

4) Technological feasibility

- *Is the technology ready to meet expectations?*
- *Are there technologies, or combinations of technologies, that should be favoured? Ruled out?*

5) Biometrics and the law

- *Is the current legal framework adequate? What adjustments would be necessary?*
- *Is it enforceable?*

6) The governance dimension

- *Is a single national approach possible? Or, is this a matter best dealt with jurisdiction by jurisdiction and program by program?*
- *Are existing political and legal oversight and accountability mechanisms adequate? Or do new ones need to be created?*
- *How important is international harmonisation of design and execution?*

7) Financial and administrative capacity

- *Is a system of biometrics-enabled citizenship and immigration documentation financially and administratively feasible?*

8) Biometric-enabled cards – assembling the package

- *Putting all the elements together, what would a successful system of biometrics-enabled citizenship and immigration documentation look like?*
- *Should such a system of documentation be mandatory? If so, can it be implemented on a basis of voluntary compliance?*

The background paper prepared by the Public Policy Forum can be accessed at:

http://cic-forum.ca/english/background.pdf

For a hard copy, please contact the Public Policy Forum at:

Public Policy Forum
1405 – 130 Albert St.
Ottawa, Ontario K1P 5G4
Tel.: (613) 238-7160
Fax: (613) 238-7990

ANNEX VI: SUMMARY OF INSTANT POLLING

At the beginning and at the end of the second day of the Biometrics Forum, participants had the opportunity to provide instant feedback on a number of questions and issues, using technology from Sharpe Decisions Inc. This Annex presents the results of this instant polling.

First Session (morning of the second day of the Forum)

A) How important is it that the Government of Canada moves to enhance the integrity of its identity documents in the next two years?

1	Not important	3%
2	Important	27%
3	Very important	52%
4	I think there are more pressing priorities.	16%

B) Given your opinion regarding the importance of enhancing the integrity of identity documents, is your current preference to move towards:

1	A more comprehensive approach, like a national identity card.	35%
2	A more incremental approach, like strengthening existing documents like the passport or drivers licence.	48%
3	Maintaining the status quo, while improving foundation documents.	11%
4	I have no opinion.	4%

C) Coming here today, which of the following best characterizes your familiarity with biometrics?

1	Very poor	3%
2	Poor	25%
3	Good	50%
4	Very good	20%

D) Which of the following best describes your interests at this Forum?

1	I work directly with biometrics.	12%
2	I am interested in its various applications from a technological point of view.	9%
3	I am primarily interested in the social implications of biometrics.	62%
4	I am interested in other applications of biometrics.	10%
5	I am not at all interested in this technology.	0%
6	None of the above.	4%

E) How serious a problem do you think the fraudulent use of identity documents is in Canada?

1	Not at all serious	1%
2	Not very serious	3%
3	Moderately serious	21%
4	Somewhat serious	25%
5	Extremely serious	35%
6	Don't know - No reponse.	12%

F) Do you personally support or oppose the use of biometrics by the federal government as a way of reducing the fraudulent use of identity documents?

1	Strongly oppose	4%
2	Somewhat oppose	17%
3	Neither	4%
4	Somewhat support	28%
5	Strongly support	44%

G) Given the growing concerns about verifying the identity of individuals, how likely do you think it is that by the end of the decade, almost every Canadian adult will have at least one biometric ID on file to verify their identity?

1	Not at all likely	1%
2	Not very likely	1%
3	Somewhat likely	8%
4	Very likely	83%
5	Don't know	5%

Second Session (afternoon of the second day of the Forum)

H) Given the growing use of biometrics by both the public and private sectors, some people believe that governments should be dealing with regulatory issues related to the use, storage and sharing of this type of information. Which one of the following statements best reflects your views?

1	Governments should deal with the regulatory issues	55%
2	There are too many risks associated with biometrics	6%
3	More information on what this means needs to be communicated	38%

I) Which of the following statements best reflects your views?

1	Biometrics have the potential to reduce millions of dollars in lost revenues due to the use of fraudulent identity documents. We owe it to ourselves to take a serious look at this technology.	51%
2	Organized crime is very advanced, particularly elements involved in the manufacture and trafficking of illegal documents, it will only be a matter of time before they can circumvent this technology.	25%
3	Don't know - No reponse.	23%

J) Which of the following statements best reflects your views?

1	I could accept the use of biometrics in a Citizenship and Immigration context, if the government provided a solid case for how it would be protected from abuse and misuse.	72%
2	Given that there have been numerous examples of how governments have lost or mishandled secret personal information, no one should have to provide this type of personal information including newcomers to Canada.	12%
3	Don't know - No reponse.	15%

K) Which of the following statements best reflects your views?

1	Documents that are used to establish identity are lost or stolen every day. If biometric information fell into the wrong hands it would represent an even greater threat to individual privacy.	27%
2	Stealing an individual's identity has become increasingly easy. Using biometric technologies will make it harder for criminals to duplicate or misrepresent current identity documents and would actually improve the protection of personal information.	62%
3	Don't know - No response	9%

L) Which of the following statements best reflects your views?

1	It makes sense to implement biometrics but only for those who stand to benefit from the technology, such as passengers who provide an iris scan to move quickly through airport security.	9%
2	The security benefits of implementing biometrics would be lost if it were implemented on a voluntary basis.	15%
3	Other issues need to be considered before detailing with mandatory or voluntary enrollment.	74%

M) Which of the following statements best reflects your views?

1	Given global realities, all individuals wishing to come to Canada, either as a refugee or an immigrant, should provide biometric identifiers with their applications.	36%
2	It would be unfair to single out newcomers to Canada. The problems of fraudulent ID are more pervasive and require a more comprehensive response.	54%
3	Don't know - No response.	9%

N) How important is it that the Government of Canada move to enhance the integrity of its identity documents in the next two years?

1	Not important	0%
2	Important	19%
3	Very important	61%
4	I think there are more pressing priorities.	19%

O) Given your opinion regarding the importance of enhancing the integrity of identity documents, is your current preference to move toward :

1	A more comprehensive approach, like a national identity card.	23%
2	A more incremental approach, like strengthening existing documents – such as the passport or driver's licence.	56%
3	Maintaining the status quo, while improving foundation documents.	20%
4	I have no opinion.	0%