Information
and Privacy
Commissioner/
Ontario

Statement to the House of Commons Standing Committee on Citizenship and Immigration regarding Privacy Implications of a National Identity Card and Biometric Technology

Ann Cavoukian, Ph.D.
Commissioner

November 4, 2003

Information and Privacy
Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

This publication is also available on the IPC website.
Cette publication est également disponible en français.

Statement to the House of Commons Standing Committee on Citizenship and Immigration regarding Privacy Implications of a National Identity Card and Biometric Technology

Thank you very much for inviting me to share my perspective on the concepts of a national identity card and biometric technology. The introduction of a national identity card, particularly if associated with one or more biometrics, will have profound implications for the citizens of this country. As the Information and Privacy Commissioner of Ontario, I am pleased to provide my perspective on these important issues.

At the outset, I would like to make a clear distinction between a national identity card and biometric technology. These are two distinct concepts.

In my opinion, the introduction of a national identity card must be supported by a clear business case, as it will be associated with a distinct set of potential advantages and disadvantages. These must be considered separately from the question of whether to add a biometric identifier to the card. Current biometric technology provides a method of authenticating individuals and, in the future when the technology improves in the accuracy of identifying an individual from a group of many candidates, it can be employed in a number of ways – not just through a national identity card. However, no matter the vehicle, biometrics pose a separate and unique set of challenges and could have a potentially lasting and corrosive effect on our society.

In my comments today, I will be concentrating on the privacy questions that would need to be answered before government institutions should consider designing or deploying biometrics, whether in combination with a national identity card, or with any other program.

Mr. Robert Marleau, Interim Privacy Commissioner of Canada, has already made an excellent presentation to this committee regarding the privacy concerns associated with a national identity card, including the marginal benefits and significant costs, both financially and in terms of our liberal democratic values. There is no need for me to cover ground that the federal Commissioner has dealt with so thoroughly.

However, I would like to only take a few moments to underscore some of the key points made by Mr. Marleau.

A business case still has not been presented to the Canadian public that provides a detailed analysis of the costs of such a program. I note that the Committee has heard evidence that the cost could range from $5- to $7-billion. A program of this magnitude and expense must therefore be supported by clear benefits. It is apparent from reviewing the submissions to the Committee that this work remains to be done.

As well, a national identity system, with the attendant huge databases and inevitable demand for access by various departments, creates significant privacy and security vulnerabilities. If Microsoft and the Pentagon can be hacked into, this must be considered as part of the risk-benefit analysis. This includes the potential misuse or compromise of sensitive personal data by rogue employees and organized crime, and of great concern, the inappropriate tracking and profiling of citizens.

Whether or not Canada proceeds with a national identity card, this country will be faced with the call for the introduction and use of biometric identifiers on travel documents. The most immediate requirement comes from the United States' *Enhanced Border Security and Visa Entry Reform Act* of 2002. This law mandates that citizens of countries who are not required to obtain visas to travel to the U.S. must have machine-readable passports with biometric identifiers no later than October 26, 2004. My understanding is that Canada is likely to receive an exemption, albeit potentially temporary, from this requirement. I would like to suggest, however, that the future need for a biometrically enhanced travel document is not a justification for a national identity card. A valid Canadian passport is sufficient to fulfil this purpose. The cost of adding a biometric to passports would be minuscule compared to developing and deploying an identity card.

However, the potential for biometric data to be added to travel documents raises the issue of how sufficient privacy protections can be designed into such a system from the start. I would like to devote the remainder of my presentation to this issue. I think you would agree that the use of biometrics is a key issue for Canadians. In fact, a study by the Massachusetts Institute of Technology identified biometrics as one of the top technologies that will change the world. For that reason, I would like to focus on biometric identifiers; those things that measure each of us, from our face geometry or iris configuration to fingerprint swirls or the timbre of our voice.

I have always taken the approach that biometrics, if designed and implemented with privacy principles from the outset, can be deployed in a way that protects personal information and respects privacy. To achieve that privacy protective state, however, there are a number of challenges to overcome.

One of the most significant of these challenges continues to be the immaturity of the technology itself. The lack of design standards for biometrics, combined with the infancy of the industry, creates systems that are not particularly accurate. Biometrics such as fingerprint or iris scanning are claiming current error rates that are between the 1 in 1,000 and 1 in 10,000 range.[1] Facial recognition systems are much less accurate. A system that can achieve up to a 99.99 per cent accuracy rate may be acceptable for authentication. But on examination, this level of accuracy is highly problematic if millions of templates must be checked during the identification process.

A comparison of an individual's biometric against just one million templates would generate up to 1,000 false matches, false positives as they are called, depending on where you set the sensitivity level. In an airport where 100,000 people fly out each day, almost everyone would be falsely identified, if the database you are checking against is in the magnitude of the FBI fingerprint database, some 46 million fingerprints. This sounds large, but for travel identification, many disparate databases will be involved, for example, Interpol, individual country watch lists, police databases, etc. What this means is that for biometrics to be effective for identification purposes, the database has to be in the thousands, not millions, of templates. Said another way, biometrics are not currently suitable for watch list identification.

To illustrate this point, I would like to quote from Bruce Schneier, a security expert and highly acclaimed cryptographer. I highly recommend Mr. Schneier's most recent book, *Beyond Fear, Thinking Sensibly About Security in an Uncertain World*, for any one engaged in the national security debate. In contemplating the use of biometrics to identify potential security threats or terrorists, Mr. Schneier said the following:

> "If you have a 1 in 10,000 error rate per fingerprint, then a person being scanned against a million-record data set will be flagged as positive 100 times. And that's every person. A system like that would be useless because everyone would be a false positive. I could build a similarly effective system much cheaper. Every time someone walks through an arch, a red light goes off. Every time. My $10 system would be just as effective at catching terrorists as your biometric system."

This illustrates the fallacy that biometrics are ideally suited for identification. The truth of the matter is that biometric systems do a great job of authentication, that is, answering the question, "Does this biometric belong to that person?" But biometrics have a much harder time answering the question, "Does this biometric belong to anyone in the database of

[1] Live tests at airports have shown error rates as high as 50 per cent. Further, a 90 per cent accuracy rate, with an average of 1 terrorist per 1 million innocent civilians, would sound 100,000 false alarms for a single terrorist. Bruce Scheier, Beyond Fear, p. 190.

terrorists or criminals?" The problem is exacerbated when the system goes outside the database of known terrorists and tries to search other loosely connected databases in order to answer the question, "Is this person a potential terrorist or threat to security?"

Significant problems are created for those citizens falsely identified in this manner. They are subject, at a minimum, to the inconvenience and embarrassment of being wrongly identified as a security threat. This inconvenience and embarrassment can lead to more serious consequences. Significant delays in flying plans can be costly, both in human and financial terms. The individual may be subjected to interrogation, which may take a physical and emotional toll. Also, we must recognize the difficulty of convincing security staff that the biometric match is incorrect and that you have been falsely accused. This is a legitimate risk, especially in any public safety or national security context where secrecy is the operative paradigm.

In addition to the problems created for a significant number of innocent individuals, consider the practical problems of a large number of false positives for airport security. Staff and facilities are required for the secondary screening of these falsely targeted individuals. Also, the high number of false positives numbs the security personnel looking for matches against data sets of pictures, themselves often of poor quality.

It is also necessary to consider the impact of inaccurate screening processes on international travel and commerce. Cross-border travel and trade is the lifeblood of the Canadian economy. The confusion and congestion caused by thousands of individuals being falsely identified on a daily basis as security risks would threaten to bring our travel and trade with other countries, particularly the United States, to a grinding halt.

This issue of every-day Canadians being falsely identified as security threats shows the importance of building due process into any biometric system. Individuals need to have a quick and ready means to establish their true identity and to disprove the biometric match that has taken place. Due process considerations are crucial to protecting not only privacy rights, but broader civil rights as well.

We must also be aware of the serious consequences associated with a system of biometrics being compromised. We are all aware of situations where systems have failed inelegantly, leaving sensitive personal information unsecured and exposed. While it is possible to change a social insurance number if it is compromised, this is far more difficult with a biometric identifier that is static and limited. We only have so many fingers or eyes for re-enrolment.

The ability to trick a biometric system is also very real. Recently, gelatin from a simple gummy bear was warmed up to receive the imprint of a fingerprint and then used to beat finger-scanning biometric technology. It would be dangerous to assume that any future biometric system would not be compromised by similar innovative, yet simple, attacks. For example, with iris scanning, we can look forward to designer contact lenses that will prevent positive identification or permit false identification.

One of the more misunderstood justifications for biometrics relates to identify theft. I say this because an argument in favour of introducing identity cards and using biometrics is that there will be a reduction in identity theft. However, consider a different approach to this issue.

Any unique identifier, such as a biometric, held in a database and used to link disparate pieces of personal information, may increase the risk of identity theft. One reason is that a biometric is the equivalent of an unchangeable PIN. Once a biometric is compromised and used to steal an identity, the time and effort to reassert an innocent victim's identity will stretch far beyond the 14-month norm for clearing up a relatively simple identity theft resulting from the theft of a PIN and credit card information. As well, if a hacker steals personal information from an identity system, reports his identity card as lost and then re-enrolls using the stolen information plus his own biometric, the hacker has obtained a completely valid card, certified by his biometric. The payoff for the thief in acquiring an identity with a biometric is therefore that much greater.

Another concern that needs to be addressed is the potential for a biometric to become a *de facto* national identity system. Unless different numbers are generated from a person's biometric information for the different services that he or she accesses, the ability to track individuals is substantial. The use of the same biometric across government programs may result in the same privacy-invasive practices as a national identity card.

An additional challenge is to prevent "function creep." This is the use of personal information for purposes not considered at the time of collection. This is a violation of the most basic tenets of privacy protection.

Take the case of the City of London, England. In an effort to reduce traffic congestion, the City introduced a five-pound sterling "congestion charge." To enforce the collection of the congestion charge, the city uses hundreds of digital video cameras and character-recognition software to ensure every driver pays. This is, by any standard, a laudable goal. But, just before the system was launched, it was discovered that the images gathered would be also be given to police and the military to search for terrorists and criminals. There is a fundamental lack of accountability in this case that could have been remedied through public discussion and debate. I would ask you to consider the grave consequences to personal privacy if a national biometric database, assembled for travel security, was then expanded, away from the public eye, and used for other, less legitimate, purposes.

One of the myths of biometric systems is that once a person is enrolled, security threats can be identified and public safety is ensured. Quite the contrary is true. As has been demonstrated in the past, terrorists and individuals who are security threats will be legitimately enrolled and will acquire authentic identification documents. As a result, a false sense of security may be created. Thanks to the introduction of a biometric, an individual who is a true security risk may be granted a new level of access, whether to an airplane or to critical infrastructure.

Finally, we cannot discount the attractive target presented by databases with personal information linked through biometric templates. Any database designed to hunt terrorists and criminals will be irresistibly attractive to exactly those individuals. We should never underestimate the time and resources an attacker will use to break a system.

It is my opinion, and that of my office, that these issues must be addressed prior to any implementation of any biometric identifier by government. However, solutions to these problems do exist. Our office took these issues into account when we developed a standard for the use of biometrics in the Province of Ontario. Starting in 1994, when the City of Toronto contemplated using biometrics to reduce fraud in its welfare system, my office worked with the City and the Ontario Government to create a set of requirements that were then adopted in the *Ontario Works Act*. To the best of our knowledge, it represents the most rigorous legislative framework in existence for the deployment of a biometric by a government agency.

The legislation stated that, in order to deploy a biometric as part of a social assistance scheme, the following requirements must be met:

- The biometric may only be collected and used for limited and specific purposes set out in the legislation;
- The biometric may only be collected from the individual to whom it relates;
- The biometric must be stored in encrypted form;
- The original biometric information must be destroyed upon encryption;
- The stored, encrypted biometric can only be transmitted in encrypted form;
- The encrypted biometric cannot be used as a unique identifier;
- No program information is to be retained or associated with the encrypted biometric information;
- There can be no ability at the technical level to reconstruct or recreate the biometric from its encrypted form;

- There must be no ability to compare biometric images from one database with biometric images from other databases or reproductions of the biometric not obtained from the individual;

- There can be no access to the biometric database by law enforcement officials without a court order or specific warrant.

While this legislation is recognized internationally as the privacy standard for the use of biometrics, we have learned much since 1994. I would like to offer the following principles that should support the introduction of any biometric.

1. **Government needs to clearly state the problem** that it intends to solve with the use of biometrics, including the necessary business case for introducing a biometric program.

2. **Broad consultation** needs to take place, allowing the many constituencies in Canada to voice their positions and make suggestions regarding the collection and use of biometric information.

3. **Legislation** is required that defines a limited purpose for introducing biometrics. The legislation must clearly set the limits for the collection, use and disclosure of the biometric information. This is the model followed in Ontario with the *Ontario Works Act*. As in that case, legislation is critical to ensuring that biometrics are collected only for limited and specific purposes and to ward off the potential for function creep discussed above.

4. **Ensure strong, effective and independent oversight**, for example through the office of the federal Privacy Commissioner, of all processes associated with the collection and use of biometric information. The oversight body must have powers to investigate complaints and report to Parliament and Parliamentary committees to resolve privacy issues. Independent oversight would ensure that the system is audited on a regular basis and set encryption standards. As importantly, the oversight body would be responsible for ensuring that due process is included in any biometrics scheme; for example, the development of criteria that would make up a "watch list" of terrorist suspects and ensuring that innocent individuals have a process for being removed from such a list.

5. **There needs to be a comprehensive Privacy Impact Assessment** completed for each stage of such a project, together with a Privacy Threat Risk Assessment, from the conceptual through to physical deployment. Such an assessment, known as a PIA, will permit officials to identify privacy vulnerabilities and develop effective solutions to safeguard personal privacy.

6. **A comprehensive evaluation of the system to test its privacy strengths and weaknesses must be undertaken.** This evaluation should use an international standard such as the Common Criteria, which is normally used to test the security strengths and vulnerabilities of a system. The Common Criteria can also be used to test privacy. This would provide assurance that any security or privacy claims made by the system are in fact valid.

As I noted earlier in my remarks, I believe in the value of a properly designed and managed biometrics system. With the proper legislative framework, privacy design correlates and oversight, biometrics can be deployed in a privacy protective manner. However, it can become a *de facto* identity system if mishandled and deployed improperly and pose a potentially lasting corrosive effect on our society.

Thank you for the invitation to share with my thoughts on the issue of a national identity card and biometrics. I have appreciated your kind attention this afternoon. This committee is engaged in a vital public debate on a topic that will affect every Canadian. I hope that I have been of some assistance as you grapple with these concepts. I will stay engaged in this issue and offer my future assistance to the Committee in addressing this significant and far-reaching matter.

I am happy to answer any questions that you might have at this time.