PRB 06-30E

Library of Parliament Bibliothèque du Parlement

BIOMETRICS AND GOVERNMENT

Lalita Acharya
Science and Technology Division

11 September 2006

PARLIAMENTARY INFORMATION AND RESEARCH SERVICE
SERVICE D'INFORMATION ET DE RECHERCHE PARLEMENTAIRES

TABLE OF CONTENTS

Page

Page

CANADA

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

BIOMETRICS AND GOVERNMENT

INTRODUCTION

Biometrics – the automated or semi-automated use of physiological or behavioural characteristics to determine or verify identity[1] – has received increased attention since the terrorist attacks of 11 September 2001. Governments around the world are increasingly turning to biometrics in an attempt to increase security at airports and border crossings, and to produce more secure identity documents. Similarly, biometric technologies are being employed or tested in a variety of commercial applications.

This paper provides an overview and comparison of the principal biometric technologies available on the market or in development, and examines some of the concerns that have been raised about security and privacy with respect to biometrics. It also discusses the use of biometrics by some national governments around the world, including the Canadian federal government.

BIOMETRIC CHARACTERISTICS AND SYSTEMS

Any human physiological or behavioural characteristic can qualify as a biometric characteristic as long as it satisfies the following requirements:

- universality: each person should have the characteristic;

- distinctiveness: any two persons should be sufficiently different in terms of the characteristic;

[1] The dictionary definition of the noun "biometrics" (or "biometry") is "the application of statistical analysis to biological data" (See Catherine Soanes and Angus Stevenson eds., *Concise Oxford English Dictionary*, 11th Edition, Oxford University Press, Oxford, 2004, p. 136). Public policy references to biometrics, however, usually use some variation of the definition provided in the text. See, for example, Peter Hope-Tindall, *Biometric-based Technologies*, OECD, 2004, p. 10, http://appli1.oecd.org/olis/2003doc.nsf/43bb6130e5e86e5fc12569fa005d004c/d15c6d3ea769bc64c1256e84004c42fc/$FILE/JT00166988.PDF.

- permanence: the characteristic should be sufficiently invariable over a period of time; and

- collectability: the characteristic can be measured quantitatively.

There are several other factors that should be considered when deciding whether or not to use a biometric-based personal recognition system, including:

- performance: the recognition accuracy and speed of the system; the resources required to achieve the desired recognition accuracy and speed; and the operational and environmental factors that affect the system's accuracy and speed;

- acceptability: the extent to which people are willing to accept the use of any given biometric technology for identification purposes; and

- circumvention: how easily the system can be fooled via fraudulent methods.(2)

In a biometric system, hardware scans and records the characteristic in question, and software interprets the data and determines the acceptability of the individual (human operators may also have a role in determining acceptability, depending on the system involved). These systems operate on three levels: i) a sensor takes an observation of the biometric characteristic; ii) the system describes the observation mathematically and produces a biometric signature; and iii) the computer inputs the biometric signature into an algorithm and compares it to one or more biometric signatures stored in the system's database.(3)

Biometric systems may operate in either verification or identification mode. In verification (or "one-to-one") mode, the system verifies the identity of the individual in question. The system validates a person's identity by comparing the captured biometric data with the individual's own biometric template(s) stored in the system's database (or on a "smart card" carried by the individual). Identity verification is usually employed for positive recognition, where the aim is to prevent multiple people from using the same identity. In verification mode, a crucial step in building an effective biometric system is enrolment. During this step, each user provides a sample of the biometric characteristic in question (by interacting with the scanning hardware). The system then extracts feature information from

(2) Anil K. Jain, Arun Ross, and Salil Prabhakar, "An Introduction to Biometric Recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 14, No. 1, January 2004, http://www.csee.wvu.edu/~ross/pubs/RossBioIntro_CSVT2004.pdf.

(3) Ravi Das, "An Introduction to Biometrics," *Military Technology*, July 2005, pp. 20-27.

the sample and stores the resulting data as a template. The user interacts with the system again to verify that the data corresponds to the template. If no match is made, the process is repeated until a match is registered and enrolment is complete.

In identification (or "one-to-many") mode, the system recognizes an individual by searching all of the templates in the database for a match. Since many comparisons are made in identification mode, the likelihood of a coincidental match, or more than one match, is possible. Identification is a critical component in applications such as "watch lists" where the system establishes whether the biometric template for an individual exists in its database.

OVERVIEW AND COMPARISON OF BIOMETRIC-BASED RECOGNITION SYSTEMS

A variety of biometric technologies are either commercially available or in the research and development (R&D) stage. Some of the more common biometric technologies include those that are used for fingerprint, face, iris and hand or finger recognition. Biometric technologies that are in less frequent use include those employed for the recognition of retinal images, gait, and dynamic signature patterns. An overview of 4 of the most widely used biometric recognition systems, and a comparison of 15 biometric techniques that are commercially available or in development are presented below.[4]

A. Fingerprint Recognition

The manual comparison of fingerprint patterns and ridges by police departments to recognize individuals has been performed since the late 1800s. In the late 1960s and early 1970s, the United States Federal Bureau of Investigation (FBI) began funding the R&D of technologies, which resulted in the development of a semi-automated system for fingerprint recognition. Technological advances have led to the availability of rapid, completely automated, commercial fingerprint systems for verification purposes. Fingerprint systems that are used for large-scale identification ("one-to-many") purposes require information from all 10 fingers (rather than just 1), and human examiners are necessary in some cases for the final comparison of fingerprints. The sensor used to collect the digital image of a fingerprint surface can be optical (the most commonly used), capacitive, ultrasonic or thermal in nature.

[4] For a detailed, technical summary of major biometric technologies see the Web page of the U.S. National Science and Technology Council's Subcommittee on Biometrics, http://www.biometricscatalog.org/NSTCSubcommittee/BiometricsIntro.aspx.

Recognition via fingerprints is highly accurate, difficult to circumvent (for sophisticated systems) and generally inexpensive. The technology is not unobtrusive, however, and there is some stigma attached to providing fingerprints because of links between the technology and the criminal justice system.

B. Face Recognition

Early face recognition algorithms used simple geometric models. The first semi-automated face recognition system was developed in the 1960s. It required the administrator to locate features (such as eyes, ears, nose, and mouth) on the photographs before the system measured distances and ratios to a common reference point, which were then compared to reference data. Today's automated face recognition technologies employ sophisticated mathematical representations and matching processes.

The verification performance of commercially available face recognition systems depends on how the facial images are obtained. These systems have difficulty in recognizing a face from images captured from two drastically different views and under different illumination conditions. Some analysts question whether the face itself, without any contextual information, is a sufficient basis for recognizing a person with an extremely high level of confidence from a large number of identities.[(5)]

C. Iris Recognition

The iris is a muscle within the eye that regulates the size of the pupil, controlling the amount of light that enters the eye. Every iris has a highly detailed and unique texture whose striations, pits and furrows allow for recognition of individuals. Automated iris recognition systems are relatively recent – the first patent for the algorithm was issued in 1994, and the first commercial products became available in 1995. These systems work by illuminating the iris with near infrared light (which is harmless to the eye) and then taking a picture of the iris with a high-quality digital camera. The random patterns within the iris are then encoded mathematically, and the resulting "iris codes" are compared statistically to one or more templates.[(6)]

[(5)] See, for example, Anil K. Jain, Arun Ross, and Salil Prabhakar, 2004.

[(6)] John Daugman, Iris Recognition for Personal Identification, http://www.cl.cam.ac.uk/~jgd1000/iris_recognition.html.

Since it is difficult to surgically alter the iris and artificial irises (e.g., contact lenses) are easy to detect, it is relatively difficult to circumvent an iris recognition system. Such systems are very accurate[7] (as long as enrolment is successful) and fast, with results obtained in a matter of seconds. One of the drawbacks of iris recognition systems is that they are not widely accepted by the public as a recognition tool largely because of (unfounded) fears that infrared light can damage the eye.

D. Hand/Finger Recognition

Hand geometry biometric recognition systems have been on the market since the 1980s, and are in use in hundreds of locations around the world. These systems measure and record the length, width, thickness, and surface area of an individual's hand. A camera captures an image of the hand from above, and angled mirrors allow a side image to be taken as well. A verification template is created and compared to the template created at enrolment.

Hand geometry systems are widely employed because they are easy to use, widely accepted by the public, and are relatively inexpensive. One of the disadvantages of the hand geometry characteristic is that it is not unique, thus limiting the applications of such systems to verification, rather than identification tasks.

E. Comparison of Biometric-based Recognition Systems

A number of other biometric techniques are either commercially available or in the R&D stage. A comparison of 15 biometric identifiers based on 7 factors is presented in Table 1 (for a description of the factors presented in the table see the earlier section entitled "Biometric Characteristics and Systems").

[7] Tests of the Daugman Iris Recognition Algorithms, http://www.cl.cam.ac.uk/~jgd1000/iristests.pdf.

TABLE 1

Comparison of Various Biometric Technologies
(H = High, M = Medium and L = Low)

Biometric identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial thermogram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Palmprint	M	H	H	M	H	M	M
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Source: Anil K. Jain, Arun Ross, and Salil Prabhakar, "An Introduction to Biometric Recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 14, No. 1, January 2004, http://www.csee.wvu.edu/~ross/pubs/RossBioIntro_CSVT2004.pdf.

TECHNOLOGICAL LIMITATIONS OF BIOMETRIC SYSTEMS

A. Accuracy of Biometric Systems

The accuracy of a biometric recognition system is characterized by two error statistics:

(i) the false rejection rate, where the system identifies two biometric measurements from the same person as being from two different persons; and

(ii) the false acceptance rate, where biometric measurements from two different persons are identified as being from the same person.

These two error statistics are related, and there is a trade-off between the two rates in every biometric system. Both rates are functions of the system's "decision threshold" – a value determined by the system's designer or operator that defines when a match is declared. Scores above the threshold value are designated as a "match" and scores below the threshold are designated as "non-match." If the threshold is decreased to make the system more tolerant to input variations and noise, then the false acceptance rate increases. On the other hand, if the threshold is raised to make the system more secure, then the false rejection rate increases. The point at which a system's false rejection rate is equal to the false acceptance rate is known as the equal error rate. The smaller this rate, the more accurate the system as it indicates a good balance in sensitivity. Besides the above error rates, the failure-to-capture rate and the failure-to-enrol rate are also used to summarize the accuracy of a biometric system.(8)

Accuracy claims provided by equipment vendors must be carefully scrutinized since (i) only one of the statistics described above may be cited by vendors to support their claims; (ii) accuracy rates provided by vendors generally have been determined from tests or operations with small-scale recognition systems under controlled conditions; and (iii) the accuracy requirements of a biometric system are dependent on whether the system is being used for verification or for identification.

B. Vulnerability of Biometric Systems

Biometric systems may be comprised either by design or by accident. Systems are vulnerable to damage or attacks at the level of the device or associated equipment at the user interface, and at the level of the system. Devices may be vulnerable to spoofing (circumvention by an impostor); environmental degradation or physical attacks; and damage to cables, wires and other communication conduits. At the level of the system, algorithms and templates may be susceptible to hacker attacks; data may be vulnerable to deletion, alteration or theft at the administrator- or account-level; and software components (e.g., drivers) may be vulnerable to attacks. Employing multimodal biometric systems that use several technologies and data from multiple biometric characteristics is one method of dealing with some of the accuracy and vulnerability limitations described above.

(8) *Ibid.*

It should also be noted that in terms of verifying identity, biometrics can only confirm that the person being inspected is the same person that enrolled in the system; if that individual used bogus “foundation” documents (e.g., birth certificates) to enrol, the system will not confirm the true identity of the person.

OTHER CONCERNS ABOUT BIOMETRIC SYSTEMS

A. Privacy Issues

1. Mass Surveillance and Related Concerns

Many civil liberties advocates object to the use of biometrics (and other recognition tools) because they see them as part of an increasing trend towards a “surveillance society” in which governments and private corporations are collecting increasing amounts of personal data, sometimes without justification. These advocates suggest that governments should not be tracking individuals or violating privacy unless there is evidence of wrongdoing.[9] A related concern with respect to some biometric-based systems (e.g., facial recognition) is that surveillance can be conducted without the consent or even the knowledge of the individuals involved.

2. Function Creep

Another privacy concern expressed about biometric-based recognition systems relates to “function creep,” which is the term used to describe the expansion of a process or system in which data collected for one specific purpose is subsequently used for another unintended or unauthorized purpose. An example of function creep is the use of Social Security numbers in the United States. In the 1930s, when these numbers were first issued, the government made assurances that the numbers would be used only to keep track of a person’s contributions to or eligibility for benefits from the Social Security system. Today, however, Social Security numbers are used widely by U.S. government agencies and private corporations to identify individuals, and they are often stolen by individuals involved in identity theft. Federal legislation to restrict the use of Social Security numbers has been enacted or proposed to help curb this activity.[10]

[9] See, for example, Jay Stanley and Barry Steinhardt, *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society*, American Civil Liberties Union, January 2003, http://www.aclu.org/FilesPDFs/aclu_report_bigger_monster_weaker_chains.pdf.

[10] For example, the *Intelligence Reform and Terrorism Prevention Act of 2004* prohibits states from displaying Social Security numbers on drivers’ licences or motor vehicle registrations.

3. Outdated Privacy Legislation

Some privacy advocates note that increased surveillance with new technologies by governments (and private corporations) has not been accompanied by changes to legislation to ensure that privacy is being protected. In Canada, for example, the *Privacy Act* places obligations on some 150 federal government departments and agencies to respect privacy rights by limiting the collection, use and disclosure of personal information.[11] The Act, which came into force in 1983, has not been substantially amended since its introduction. The Privacy Commissioner of Canada has stated that, because of technological and other changes, the privacy landscape has changed radically over the last 20 years and the Act is an "… outdated law that leaves the Office of the Privacy Commissioner of Canada virtually powerless to protect the privacy rights of Canadians relating to information collected, used and disclosed by the federal government …."[12]

The Office of the Privacy Commissioner is not opposed to the use of biometrics under the appropriate circumstances. The Office believes that biometric-based recognition tools, when properly handled, can actually enhance individuals' privacy and control of their own identity. However, misuse of biometrics can lead to "undesirable" privacy invasions. The Office examines the use of biometrics on a case-by-case basis. It believes that "any privacy-invasive measure being proposed must be demonstrably necessary in order to meet some specific need, it must be likely to be effective in achieving its intended purpose, the intrusion on privacy must be proportional to the security benefit to be achieved and it must be demonstrable that no other, less privacy-intrusive measure would suffice to achieve the same purpose."[13]

B. Implementation and Operating Costs

Another concern about employing biometrics as a recognition tool is the cost of implementing and running these systems. Although some biometric systems used in corporate settings on a small scale may be relatively inexpensive to install and maintain, the lifetime cost

[11] In Canada, individuals are also protected by the *Personal Information Protection and Electronic Documents Act* (PIPEDA) that sets rules for how private sector organizations may collect, use or disclose personal information in the course of commercial activities.

[12] Office of the Privacy Commissioner of Canada, "Privacy Commissioner tables report calling for urgent reform of Canada's *Privacy Act*," News release, 5 June 2006, http://www.privcom.gc.ca/media/nr-c/2006/nr-c_060605_e.asp.

[13] Personal communication with the Office of the Privacy Commissioner of Canada. Information from media lines provided in July 2006.

of other, more sophisticated systems intended for large-scale operations may be prohibitive for some operators (including governments). Costs for such systems include not only the initial capital expenditures for hardware and software, but also costs for issuing identity documents (in some cases), training and employing staff, maintaining equipment and managing databases.

USE OF BIOMETRIC SYSTEMS BY WORLD GOVERNMENTS

Various governments around the world are either employing or considering deploying biometric-based systems for identification and verification purposes. A survey of some of the major systems (or programs) in use or under development by national governments in the United States and the United Kingdom, and by Member States of the European Union is presented below. The situation in Canada with respect to the employment of or plans for biometric-based recognition by the federal government is also discussed.

A. United States

Not surprisingly, given increased security concerns, the United States government is a world leader in the introduction of biometric-based technologies for verification and identification purposes. It already has several programs and systems in use or planned that employ biometrics, and some of the major ones are described below:

1. Integrated Automated Fingerprint Identification System (IAFIS)

The U.S. Department of Justice's FBI maintains the IAFIS, an automated 10-fingerprint matching system that captures rolled prints. The IAFIS became operational in 1999 and, with fingerprints for more than 47 million subjects on file, it is the largest biometric database in the world.[14]

2. United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program

The US-VISIT program, established by the Department of Homeland Security (DHS) and launched in 2004, collects, maintains, and shares information, including biometric identifiers, on selected foreign nationals[15] entering and exiting the United States. US-VISIT

[14] Federal Bureau of Investigation, http://www.fbi.gov/hq/cjisd/iafis.htm.

[15] Most Canadian citizens are currently exempt from the US-VISIT program, http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0695.xml.

uses digital finger scans and photographs to screen persons against watch lists (of criminals, terrorists and immigration violators), and to verify that a visitor is the person who was issued a visa or other travel document. Visitors also confirm their departure by having their visas or passports scanned and by undergoing finger scanning at selected air and sea ports of entry. Biometric data are stored in the Automated Biometric Identification System (IDENT) database, and include fingerprint information from the FBI's IAFIS. Full integration between IDENT and IAFIS is a goal.

The program has come under attack from the U.S. Government Accountability Office (GAO), which says that the DHS has been very slow in assessing and testing basic system security and privacy controls. The GAO also noted that the DHS had not demonstrated that the program is producing or will produce "mission value commensurate with expected costs and risks." In particular, the department's return-on-investment analyses for exit processes were singled out as not demonstrating that these exit procedures will be cost-effective.(16)

3. Registered Traveler (RT) Program

The RT Program is under development by the DHS. The program will be a voluntary, fee-based, market-driven initiative offered by the private sector with government oversight. The program's goal is to "strengthen aviation security and enhance customer service." Companies that enrol participants in the program will collect fingerprints and iris biometrics and basic biographic information from applicants (e.g., frequent flyers). Information collected will then be analysed by the DHS to conduct "threat screening" in advance of travel for individuals participating in the program. Individuals who participate in the program will, in theory, be provided with expedited screening at the airport. Government-operated pilot programs for RT ran in five US airports in 2004 and 2005, and an evaluation of these pilots deemed the program to be "viable."(17) A public-private partnership pilot was also conducted at the airport in Orlando, Florida. A national rollout of the RT program was originally scheduled for June 2006, but the Web site of the Transport Security Administration (TSA) states that implementation will begin later in 2006.(18)

(16) United States Government Accountability Office, *Homeland Security: Recommendations to Improve Management of Key Border Security Program Need to Be Implemented*, February 2006, http://www.gao.gov/new.items/d06296.pdf.

(17) United States Department of Homeland Security, Transportation Security Administration, Statement of Kip Hawley, Assistant Secretary before the Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity, Committee on Homeland Security, United States House of Representatives, 3 November 2005, http://www.tsa.gov/assets/pdf/110305TRAV.pdf.

(18) United States Department of Homeland Security, Transportation Security Administration, Registered Traveler, http://www.tsa.gov/what_we_do/layers/rt/index.shtm, site accessed 6 September 2006.

Various groups are opposed to the RT program. The Air Transport Association of America states that "the program will unnecessarily drain limited TSA resources and detract from the agency's ability to craft more comprehensive programs benefiting all travelers."[19] The American Civil Liberties Union suggests that the initiative would force Americans to choose between preserving their most private and personal information and speeding through airport security. Furthermore, the group argues that the program could make the United States more vulnerable to terrorist attacks since terrorists could enrol in the program by using fake identification.[20]

B. United Kingdom

In 2006, the British Parliament passed legislation[21] to introduce biometric-based national identity (or ID) cards. The government has touted the cards as a means to reduce identity fraud, reduce illegal immigration to the United Kingdom, and help in the reduction of organized crime and terrorism, among other benefits. Under a timetable set out when the legislation was passed, from 2008 onwards, everyone renewing a passport will be issued an ID card and have his or her personal information (including biometric data) placed in an associated database – the National Identity Register. The biometric portion of the system will likely use face recognition, fingerprints and iris scans. Later on, the government plans to introduce stand-alone identity cards for people who do not want a passport. Until 2010, people can choose not to be issued a card, though they will still have to pay for one, and will still be placed in the database. Possessing an identity card will eventually become compulsory.

Concerns related to the accuracy and vulnerability of biometric systems have been raised with respect to the national identity cards scheme. A report[22] released by researchers at the London School of Economics and Political Science (LSE) prior to the passage of the

[19] Air Transport Association, Open letter, June 2006, http://www.airlines.org/files/AirportDirectorsLetter.pdf.

[20] Testimony of Timothy D. Sparapani, ACLU Legislative Counsel, On Secure Flight and Registered Traveler Before the U.S. Senate Committee on Commerce, Science and Transportation, 9 February 2006, http://www.aclu.org/safefree/general/24113leg20060209.html.

[21] Identity Cards Act 2006, http://www.identitycards.gov.uk/downloads/ukpga_20060015_en.pdf.

[22] LSE Identity Project 2005, *The Identity Project: an assessment of the UK Identity Cards Bill and its implications*, London School of Economics and Political Science, June 2005, http://is2.lse.ac.uk/idcard/identityreport.pdf.

legislation suggested that the technology at the core of the scheme has been untested on the scale proposed by the United Kingdom's Home Office, and that the database with the details of every ID card holder is likely to become a major target for security attacks. Another report, by a House of Commons committee, noted that there was a lack of transparency surrounding the incorporation of scientific advice, and that "choices regarding biometric technology have preceded trials."[23]

Although there are privacy concerns related to the identity cards proposal, much of the criticism of the scheme has centred on its cost. For example, the LSE report estimated that the scheme's implementation and running costs would be in the range of £10.6 billion to £19.2 billion (approximately C$22.3 billion to $40.4 billion) over the first 10 years (at 2005-2006 prices).[24] This estimate is considerably higher than the government's estimate of £584 million a year.[25] In response to the LSE report, the Home Office branded the LSE's cost estimates as being "vague" and based on "misguided assumptions,"[26] and provided an excerpt from another review that suggested that the methodology for the government's cost estimates was robust.[27] The government later clarified that its figure applied only to the annual operating cost of the scheme for the lead department (the Home Office). Although the government has not provided a final estimate of the total cost of the scheme, because it deems that information to be "commercially sensitive," the legislation requires the government to provide an estimate to Parliament every six months on the public expenditure likely to be incurred on the ID cards scheme.

Recent news reports and statements from the Home Office suggest that the identity cards scheme, at least in its present form, may be in trouble. According to these reports, the timetable for introduction of the cards is under review as part of an examination of all

[23] House of Commons Science and Technology Committee, *Identity Card Technologies: Scientific Advice, Risk and Evidence*, Sixth Report of Session 2005-2006, August 2006, http://www.publications.parliament.uk/pa/cm200506/cmselect/cmsctech/1032/1032.pdf.

[24] LSE Identity Project 2005.

[25] UK Home Office, *Regulatory Impact Assessment*, May 2005, http://www.identitycards.gov.uk/downloads/Identity_cards_bill_regulatory_impact.pdf.

[26] UK Home Office, Home Office Response to The London School of Economics' ID Cards Cost Estimates & Alternative Blueprint, July 2005, http://www.identitycards.gov.uk/downloads/Response_LSE_Alternative_Blueprint.pdf.

[27] KPMG, *Home Office ID Cards Programme Cost Methodology and Cost Review Outline Business Case Review*, Published Extract, November 2005, http://www.identitycards.gov.uk/downloads/2005-11-7_KPMG_Review_of_ID_Cards_Methodology.pdf.

Home Office operations.[(28)] The British Prime Minister has stressed, however, that the initiative will go ahead, and that it is a major plank of the Labour Party's manifesto for the next U.K. general election.[(29)]

C. Member States of the European Union

Likely in response to (non-binding) standards set by the International Civil Aviation Organization (ICAO), an agency of the United Nations, and requirements put in place by the U.S. government for its US-VISIT Program, Member States of the European Union (EU) have begun including biometric identifiers in passports. Under the US-VISIT program, as of 26 October 2006, the 27 countries that are participating in the U.S. visa waiver program[(30)] must issue machine-readable "e-passports." These passports must contain an integrated computer chip capable of storing biographic information from the data page, a digitized photograph, and other biometric information.[(31)] The ICAO endorses the use of standardized, digitally-stored facial images as the globally interoperable biometric for machine-assisted identity verification. It has selected high-capacity, contactless integrated circuit chips (that operate at radio frequencies) to store identification information in machine-readable travel documents as the standard for storage devices.[(32)]

In 2004, the European Commission issued a regulation (that is binding for all Member States except the United Kingdom and Ireland[(33)]) that sets out minimum security standards for passports and travel documents.[(34)] The regulation stipulates that passports and travel documents shall include a storage medium which shall contain a facial image, and that the

[(28)] See, for example, Richard Ford, "ID cards under threat in review of Home Office," *Times Online*, 12 July 2006, http://www.timesonline.co.uk/article/0,,2-2266071,00.html.

[(29)] Prime Minister Tony Blair's monthly press conference, August 2006, http://www.pm.gov.uk/output/Page9960.asp.

[(30)] See a description of the program and the list of participating countries at http://travel.state.gov/visa/temp/without/without_1990.html#2.

[(31)] US Visa Waiver Program, Timelines 2005-2006, http://cbp.gov/linkhandler/cgov/travel/id_visa/vwp/vwp_timeline.ctt/vwp_timeline.pdf.

[(32)] Doc 9303 Specifications for Machine Readable Travel Documents, http://www.icao.int/mrtd/publications/doc.cfm.

[(33)] The United Kingdom and Ireland have not signed the *Schengen Convention*.

[(34)] Council Regulation (EC) No 2252/2004 of 13 December 2004 on Standards for Security Features and Biometrics in Passports and Travel Documents Issued by Member States, http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_385/l_38520041229en00010006.pdf.

documents shall also include two fingerprints in interoperable (across the EU) formats. All Member States had until 28 August 2006 to implement the facial image requirement, and have until 28 June 2009 to implement the fingerprint requirement.

Critics of the EU's planned biometric passports scheme note that the inclusion of a digitized photograph in passports meets the standards set by the ICAO, but that the EU has gone further by requiring the inclusion of fingerprints. They also point out that since only two fingerprints will be taken, the error rate for an EU-wide database will be relatively high if it is to be used for identification (rather than just verification) purposes.(35)

D. Canada

The Canadian federal government, either alone or in collaboration with the U.S. federal government, employs biometric-based technologies in several programs. It is likely that the use of these technologies will increase, especially in light of changes to international passport standards and proposed changes to passport requirements for travel to the United States. A description of the major federal programs, departments or agencies that employ, or plan to use, biometric technologies is provided below.

1. Royal Canadian Mounted Police (RCMP)

The RCMP recently began upgrading its fingerprint identification system to improve its speed and accuracy. The new Automated Fingerprint Identification System (AFIS) will support the accurate processing of good-quality fingerprint submissions with little or no manual intervention. The transfer of 4 million fingerprint files from the old AFIS to the new AFIS was projected to be completed in the summer of 2006. A new server will permit the electronic exchange of fingerprint identification requests. The new systems should be in operation by the end of 2006.(36)

2. CANPASS Air

CANPASS Air is a Canada Border Services Agency (CBSA) program that is intended to facilitate "efficient and secure entry into Canada for pre-approved, low-risk air travellers." The program, which is currently available at seven Canadian airports, uses iris

(35) See, for example, Statewatch editorial, http://www.statewatch.org/news/2006/jul/04eu-bio-passports.htm.

(36) RCMP Real Time Identification Project (RTID), http://www.rcmp-grc.gc.ca/rtid/report_issue1_e.htm.

recognition technology to verify a passenger's identity. Under the program, citizens and permanent residents of Canada who wish to participate in the program undergo security checks at registration and every year upon renewal. For an annual fee (currently $50), members of the program receive an identification card that enables them to use the self-serve CANPASS Air kiosks at airports where their iris is photographed and the image compared to that stored in the database. Once their identity is confirmed, individuals then proceed to baggage claim and leave the customs premises without further interaction with a CBSA officer unless they are selected randomly for inspection.

3. NEXUS

NEXUS[37] is a group of fee-based programs operated jointly by the Canadian and U.S. federal governments that arose from the Canada-United States 30-point Action Plan of the Smart Border Declaration signed in December 2001.[38] For the three NEXUS programs – NEXUS Highway, NEXUS Marine and NEXUS Air – biometrics (fingerprints) are taken as part of the application process to perform a background check. Once approved by both Canada and the United States as low-risk travellers, NEXUS members benefit from a simplified entry process when travelling across the Canada-United States border by motor vehicle, recreational boat or aircraft.

NEXUS Air is a pilot program that began in November 2004 and operates only at the Vancouver International Airport. It offers expedited customs and immigration clearance to pre-approved, low-risk passengers travelling between Canada and the United States. The program works in a similar fashion to CANPASS Air by employing iris recognition technology to verify a passenger's identity. Once an individual's identity has been confirmed by one of the automated kiosks located in the airport, members answer either U.S. or Canadian (depending on their destination) customs and immigration questions using a touch screen at the kiosk. The kiosk then issues a receipt and members entering Canada are directed towards either the exit or the secondary inspection area. Members flying to the United States are directed to either the secondary inspection area or on to security screening.

[37] NEXUS, http://www.cbsa-asfc.gc.ca/travel/nexus/menu-e.html.

[38] Smart Border Declaration, http://www.cbsa-asfc.gc.ca/newsroom/factsheets/2002/sep/smart-e.pdf.

4. Passport Canada

Enhanced security features have been added to Canadian passports issued domestically since 2002 and since April 2006 for Canadian passports issued abroad. These features include a digital photo, holograms, special ink and a machine-readable zone at the bottom of the personal information page. Canadian passports do not currently contain biometric identifiers, but biometrics will likely be included in the newest version of the Canadian passport that is in development. In September 2004, amendments to the *Canadian Passport Order* were brought into force, two of which allow Passport Canada to include biometrics in passports.[(39)] The first amendment provides Passport Canada with the authority to convert any information submitted by an applicant into a digital biometric format for the purpose of inserting that information into a passport. The second amendment authorizes Passport Canada to convert an applicant's photograph into a biometric template for the purpose of verifying the applicant's identity.

Passport Canada is currently developing its new "e-passport." The document will meet ICAO standards, which call for the inclusion of an electronic contactless chip containing, among other items, a digital photo for facial recognition purposes. The agency has released little information publicly about the e-passport project. According to its *Corporate and Business Plan 2005-2008*, e-passport specimens were to be tested with Canadian diplomats and ministers as part of a pilot project in July 2006, and a national rollout of the documents would happen in July 2007.[(40)] The agency now says, however, that "the e-passport is at a developmental stage, and it is premature to discuss cost as well as timeframe for the launch of the e-passport project."[(41)] At present, Passport Canada is moving ahead with a separate (and it claims unrelated) project to introduce a facial recognition system to be used during the application process. The system would, when fully operational, perform identification and verification tasks, and would compare applicants' facial images to those on a watch list compiled from a variety of sources. The system would assist Passport Canada "in making and supporting entitlement and passport issuance decisions."[(42)]

[(39)] *Order Amending the Canadian Passport Order*, P.C. 2004-951, 1 September 2004, http://www.ppt.gc.ca/publications/pdfs/order_04_113.pdf.

[(40)] Passport Canada, *Corporate and Business Plan 2005-2008*, http://www.ppt.gc.ca/publications/pdfs/bp05-08_ca_e.pdf, June 2005.

[(41)] Personal communication with media relations officer at Passport Canada, 30 August 2006.

[(42)] Information from a public tender notice for a "Facial Recognition Solution" on MERX published on 14 July 2006, http://www.merx.com/English/SUPPLIER_Menu.Asp?WCE=Show&TAB=1&State=7&id=PW-%24EEM-006-14751&hcode=shsxpr2tIBMeERly4npDoQ%3d%3d.

The planned introduction of facial recognition technologies and biometric passports is being done with little or no public debate. Some critics of the process to introduce an e-passport suggest that the federal government is engaging in "policy laundering" – introducing policies developed by foreign and international fora (in this case the issuance of biometric passports that meet ICAO standards) that might not otherwise win approval through the regular domestic political process.(43)

Passport Canada has submitted a Privacy Impact Assessment on the e-passport initiative to the Office of the Privacy Commissioner. The Office is not opposed to the inclusion of biometric identifiers *per se* in passports, but does have some concerns that it says the Passport Office should address about the security of the information included on the proposed e-passport's chip. The Office has indicated that any e-passport system should protect passport holders against such activities as "skimming" and "eavesdropping." Skimming refers to the process whereby someone uses an unauthorized reader to collect the information in a passport's chip surreptitiously, such as when the passport is in someone's pocket. Eavesdropping involves someone intercepting and reading the transmission between the passport's chip and the reader.(44)

5. Other Initiatives

In 2002, the then-Minister for Citizenship and Immigration, Denis Coderre, called for a public debate on the introduction of a national identity card containing biometric identifiers. The debate occurred, in part, via hearings conducted by the House of Commons Standing Committee on Citizenship and Immigration. The Committee's interim report,(45) tabled in 2003, detailed several concerns about a national identity card system and concluded that a much broader public debate was necessary to decide on the merits of a national identity card itself. If the card were deemed necessary, the Committee noted that other issues such as the financial cost of an identity card system, the nature of the biometric technology to be employed, the security of personal data, and other privacy issues also had to be addressed. The Committee did not table a final report on the national identity card scheme. Following the June 2004 general election, the issue disappeared from the federal government's agenda.

(43) See, for example, Andrew Clement and Krista Boa, "Developing Canada's Biometric Passport: Where are Citizens in this Picture?" http://ts6.cgpublisher.com/proposals/55/index_html (site accessed 11 September 2006).

(44) Personal communication with the Office of the Privacy Commissioner of Canada. Information from media lines provided in July 2006.

(45) House of Commons Standing Committee on Citizenship and Immigration, *A National Identity Card for Canada?* October 2003, http://www.parl.gc.ca/infocomdoc/documents/37/2/parlbus/commbus/house/reports/cimmrp06/cimmrp06-e.pdf.

CONCLUSION

Given the security-conscious world in which we live, it is likely that biometric-based recognition systems are here to stay. The systems will probably become commonplace at borders, airports and other establishments where security is a concern. The International Civil Aviation Organization has set standards for machine-readable travel documents that include the inclusion of biometric identifiers; as such, "e-passports" that include biometrics will likely eventually become the only acceptable document for international travel.

Biometric-based recognition systems are privacy-intrusive security measures. For this reason, some critics object altogether to the use of these systems, whereas others note that the systems may be necessary in certain cases, but only if appropriate security and legal measures are in place to protect the sensitive personal data that are collected. Specific concerns about the use of biometric-based recognition systems include their technological limitations (related to their accuracy and vulnerability); increased, and in some cases unnecessary, surveillance of citizens' daily activities; theft or manipulation of biometric and other personal data held on centralized databases; function creep (where biometric data collected for one specific purpose is subsequently used for another unintended or unauthorized purpose); and the high cost of implementing and operating many of these systems.

The Canadian federal government, like other governments around the world, is employing or experimenting with biometrics in a number of situations. Voluntary biometric verification of passenger identity via iris recognition is already in place at several Canadian airports, and a similar joint Canadian-American program is in the pilot stage. Passport Canada is in the process of developing an e-passport (that contains biometrics), and is currently working on a facial recognition system to help it screen applicants. The Office of the Privacy Commissioner of Canada is not opposed to the use of biometrics under the appropriate circumstances, but it notes that the *Privacy Act* is in urgent need of reform to ensure that it reflects recent technological changes, including the introduction of biometrics.

Biometric-based recognition systems are potentially important tools for enhancing security in some situations. However, before governments decide whether to implement such systems, they should conduct detailed analyses to ensure that the technology is actually required, and that no other less privacy-intrusive measure would achieve the same purpose. Furthermore, the biometric technologies employed should be both efficient and used in such ways that the loss of privacy is minimized.