CANADIAN HUMAN RIGHTS COMMISSION
COMMISSION CANADIENNE DES DROITS DE LA PERSONNE

# *Identity Certification and the Protection of Human Rights*


Prepared by:

Caleb Chepesiuk
Independent Researcher

and
Maciej Mark Karpinski

Senior Research Analyst, Research and Statistical Analysis
Canadian Human Rights Commission

And

Dr. Charles Théroux
Director, Research and Statistical Analysis
Canadian Human Rights Commission



August 2010

HR4-8/2011E-PDF
ISBN: 978-1-100-18536-1

## EXECUTIVE SUMMARY

This study examines the various methods used to certify an individual's identity as a way of exploring the implications that may arise when implementing these methods on those rights protected under the *Canadian Human Rights Act* (*CHRA*). The *CHRA* seeks to protect individuals from discrimination based on a prohibited ground (race, national or ethnic origin, colour, religion, age, sex, sexual orientation, marital status, family status, disability or a pardoned conviction) in employment and in the provision of services. It is a violation to deny access to or differentiate adversely in relation to any individual based on the enumerated prohibited grounds unless there is a demonstrated justification.

The study reviews various identification methods. The actual or potential discriminatory impact of each identification method is then examined based on the enumerated grounds under the *CHRA*. For each identification method, relevant Canadian jurisprudence is surveyed concerning the discriminatory impact, including measures of accommodation or *bona fide* justifications where an accommodation was not possible.

Non-biometric and biometric measures are surveyed including a person's name, date of birth, the face, the hand, fingerprints, irises, and handwritten signatures.

The identity documents reviewed consist of the Passport, the Canadian Permanent Resident Card, CANPASS AIR and NEXUS.

The review found that most of the biometric measures have limits and may affect one or more groups protected under the *CHRA*.

The Supreme Court of Canada has indicated that employers and service providers have a duty to prevent new barriers from arising. This is to be done by developing the measure in the most inclusive way possible. Biometrics should therefore be developed in a manner that allows the largest number of individuals to participate. Where technological limits exist, alternative and/or supplemental metrics ought to be considered. Using supplemental metrics, thereby creating multi-modal systems, offers a degree of flexibility that may be able to address a number of potentially discriminatory effects. Where additional exceptions are required, policies and practices for accommodating individual differences short of undue hardship should be also considered.

The *Canadian Charter of Rights and Freedoms* and the *Canadian Human Rights Act* recognize that there may be limits to the exercise of individual rights. The responsibility, however, is on the organization employing the measure to demonstrate that the system used was designed in a manner that is consistent with human rights principles.

**TABLE OF CONTENTS**


**1. INTRODUCTION ..... 1**

**2. METHODOLOGY ..... 4**

**3. METHODS OF IDENTITY CERTIFICATION ..... 5**

3.1 NON-BIOMETRIC IDENTIFIERS ..... 8
3.2 BIOMETRIC IDENTIFIERS ..... 9
*3.2.1 Facial Recognition ..... 10*
*3.2.2 Hand Geometry ..... 12*
*3.2.3 Fingerprinting ..... 13*
*3.2.4 Iris Recognition ..... 14*
*3.2.5 Handwritten Signature ..... 15*
*3.2.6 Other Biometric Methods ..... 15*
3.3 LIMITATIONS OF BIOMETRIC METHODS ..... 16
*3.3.1 Accessibility ..... 16*
*3.3.2 Discretionary decisions based on manual inspection ..... 17*
*3.3.3 Means of mitigating biometric limitations ..... 18*

**4. THE USE OF NON-BIOMETRIC AND BIOMETRIC METHODS IN IDENTITY DOCUMENTS ..... 19**

4.1 PASSPORT, CANADIAN PERMANENT RESIDENT CARD, CANPASS AIR, NEXUS ..... 20
4.2 REQUIREMENTS OF NON-BIOMETRIC IDENTIFIERS ..... 23
4.3 REQUIREMENTS FOR THE USE OF BIOMETRIC IDENTIFIERS ..... 25
4.4 HUMAN RIGHTS LEGAL ISSUES THAT HAVE ARISEN FROM THE USE OF NON-BIOMETRIC IDENTIFIERS ..... 26
4.5 HUMAN RIGHTS LEGAL ISSUES THAT HAVE ARISEN FROM THE USE OF BIOMETRIC IDENTIFIERS ..... 26

**5. THE IMPACT OF BIOMETRICS ON HUMAN RIGHTS: TWO KEY PRINCIPLES ..... 29**

5.1 THE DUTY TO ACCOMMODATE ..... 30
5.2 A BONE FIDE JUSTIFICATION ..... 32

**6. CONCLUSION ..... 32**

**APPENDIX A ..... 35**

**BIBLIOGRAPHY ..... 36**

## 1. Introduction

The terrorist attacks in the United States on September 11, 2001, had a significant impact on Canada and Canadians. Among its numerous responses, the Canadian government implemented its first-ever National Security Policy: *Securing an Open Society*.[1] The policy is designed to "balance the needs for national security with the protection of core Canadian values of openness, diversity and respect for civil liberties." One of the eight topics covered by this policy is the issue of border security.

Along the "world's longest undefended border," border security presents many different challenges, including the complicated task of implementing new controls. Both Canada and the U.S. depend culturally and economically on an open border. Approximately 300,000 people and 35,000 trucks cross the Canadian-American border each day, as does $1.6 billion in two-way commercial trade.[2]

In addition to the National Security Policy, the Canadian government introduced the *Action Plan for Creating a Secure and Smart Border*.[3] This *Action Plan* focuses on four issues: the secure flow of people, the secure flow of goods, secure infrastructure, and coordination and sharing of information.

The issue of particular concern related to border security for the purposes of this research is the secure flow of people. On this subject, the *Action Plan* focuses largely on

The authors would like to acknowledge and thank all those federal government organizations who provided valuable feedback on an earlier version of this report.

[1] "Securing an Open Society: Canada's National Security Policy." Privy Council Office. April 2004.

[2] "A Canada–U.S. Border Vision." Canadian Chamber of Commerce. December 2008, http://www.chamber.ca/cmslib/general/blueprint.pdf.

[3] "Action Plan for Creating a Secure and Smart Border." Department of Foreign Affairs and International Trade. 2001. http://www.dfait-maeci.gc.ca/anti-terrorism/actionplan-en.asp.

identification and risk management, categorizing travellers as either low or high-risk.[4] The goal is to determine a person's risk category before they reach a border point or gate in order to facilitate the crossing of low-risk travellers, and to prevent the entry of high-risk ones.[5] The United States has additionally introduced the *Western Hemisphere Travel Initiative*, which requires all nationals to show a secure travel and identity document upon entry.

Identity documents have long been a necessity for crossing borders in most parts of the world. The increasing push for secure "smart" borders has witnessed an evolution of these documents incorporating increasingly sophisticated technologies that require the use of new identifiers in order to certify an individual's true identity. One of these technologies is biometrics. The issue of biometrics – the science and technology of measuring and analysing biological data – is part of the *Action Plan*, which states that Canada and the United States are to "jointly develop on an urgent basis common biometric identifiers in documentation such as permanent resident cards, NEXUS,[6] and other travel documents to ensure greater security."[7]

The Government of Canada has an obligation to issue the necessary documentation to those individuals who wish to travel. Concomitantly, the state has a responsibility to safeguard territorial security and the security of its citizenry. This

---

[4] See David Lyon, *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. London: Routledge, 2003; Davina Bhandar, "Renormalizing Citizenship and Life in Fortress North America." *Citizenship Studies 8* (3) Sept. 2004. 261–278; Matthew B. Sparke, "A Neoliberal Nexus: Economy, security and the biopolitics of citizenship on the border." *Political Geography* 25 (2006): 151–180.
[5] "Safety and Security: Managing access to Canada." Canada Border Services Agency. July 31, 2008. http://www.cbsa-asfc.gc.ca/security-securite/safety-surete-eng.html#s2_1.
[6] NEXUS is a joint Canada–U.S. program to facilitate border crossing for low-risk individuals. See http://www.cbsa-asfc.gc.ca/prog/nexus/menu-eng.html for more information.
[7] "Action Plan for Creating a Secure and Smart Border." Department of Foreign Affairs and International Trade. 2003. http://www.dfait-maeci.gc.ca/anti-terrorism/actionplan-en.asp.2008. http://www.spp.gov/pdf/key_accomplishments_since_august_2007.pdf.

includes the control of access into Canada and the authentication and verification of secure identity documentation to facilitate that control.[8] How the state goes about developing such security measures is partially governed by the *Canadian Human Rights Act* (*CHRA*).

The *CHRA* is quasi-constitutional. Its purpose is to give effect "to the principle that all individuals should have an opportunity…to make for themselves the lives that they are able and wish to have and to have their needs accommodated…without being hindered in or prevented from doing so by discriminatory practices."[9] It is contrary to the *CHRA* to deny access to, for example, travel documents or to differentiate adversely against an individual or group of individuals through the use of specific identity certification methods based on race, national or ethnic origin, colour, religion, age, sex, sexual orientation, marital status, family status, disability or a pardoned conviction unless there is a demonstrated justification.

This research explores the relationship between the rights of those people protected by the *CHRA* and some of the most salient methods used in identity certification processes. The objective is to determine whether there are generalizable limitations that may make identity certification methods potentially discriminatory from a human rights perspective. The paper begins with a general overview of a select number of non-biometric and biometric methods. The review is not meant to be comprehensive or exhaustive. The method is then analyzed through the prism of relevant jurisprudence as a

[8] The Government's responsibility to facilitate mobility is partially limited by the conditions for entry set by other states. "Permission to enter another country is the sole prerogative of that country." Moreover, "the right of a Canadian to leave Canada is a one sided coin. The right to enter the United States does not exist as the other side of the coin. A Canadian may practically not be able to leave Canada if no foreign country will let him enter it." (*N.B. v. Canada (Attorney General).* 27 A.R. 135, 40 C.P.C. (4th) 244. at 55.)
[9] *Canadian Human Rights Act,* R.S.C. 2009, H-6, s. 2.

means to understand the relationship between the method and the rights of those people affected. The results point to some key principles that should be considered when developing identity certification methods.

This study stems from previous research on the question of national security,[10] and focuses on the effects of technology on human rights in an evolving security environment. Privacy concerns and "function creep"[11] are within the purview of the *Privacy Act* and are thus not considered in this paper.

## 2. Methodology

This study begins with a brief literature review of a sample of non-biometric identifiers used in Canada, the United States and Britain: name, place of birth, date of birth, gender/sex, age, parents' names, criminal record status, citizenship, and identification codes. The main focus of the study, however, is on biometric methods: facial recognition, hand geometry, fingerprinting, iris scans, handwritten signatures, audio-visual and DNA testing. After a brief introduction to each biometric method, some of its limitations are addressed. The actual or potential discriminatory impact of each identification method is then examined based on the prohibited grounds of discrimination under the *CHRA*. Information used is largely obtained from industry publications, peer reviewed articles and some government sources.

[10] Wesley Wark, "National Security and Human Rights Concerns in Canada: A Survey of Eight Critical Issues in the Post 9/11 Environment." Prepared for the Canada Human Rights Commission, 2007.
[11] Function creep occurs when information used for one purpose begins to be used for other purposes.

How these methods are used is illustrated through a review of the requirement needed to obtain a Passport, the Canadian Permanent Resident Card, CANPASS AIR and NEXUS. The information for this section comes from government publications.

For each identification method presented, we survey jurisprudence concerning discriminatory impacts, including measures of accommodation or *bona fide* justifications to warrant differential treatment. The legal analysis in this section is restricted to Canadian jurisprudence.

A preliminary version of this report was circulated for consultation to the following government organizations: Department of Foreign Affairs and International Trade (DFAIT), Passport Canada, Citizenship and Immigration Canada (CIC), Public Safety, Canadian Border Services Agency (CBSA), Transport Canada, Canadian Air Transport Security Authority (CATSA), Royal Canadian Mounted Police (RCMP), Public Complaints Commission Against the RCMP, RCMP External Review Committee, Canadian Security Intelligence Services (CSIS), Office of the Inspector General (CSIS), Security Intelligence Review Committee (SIRC), Department of National Defence (DND), Communications Security Establishment Canada (CSE), the Office of the Communications Security Establishment Commissioner, the Office of the Auditor General, and the Office of the Privacy Commission.

## 3. Methods of Identity Certification

Identity certification typically involves an “identity claim” and a “token” used to verify the claim. A “token” refers to any physical object that can be used to verify an

identity claim, such as a driver's license, a door key, or a swipe card. Certifying identity or having one's identity certified is something that people do on a daily basis, from recognizing a face in the crowd to using an ATM card. A typical example is a driver being pulled over by a police officer. The officer may ask for a person's name and, in order to verify the claim, will ask to see documentation (such as a driver's license). The officer examines the presented identification by comparing the information to what the officer has been told. If there is a photo, the officer compares it to the person's face. Similarly, if the driver wants to ensure the identity claimed by the person in uniform, the driver can ask to see the officer's badge. If either of them has further doubts, the information can be checked against a database or verified with police headquarters. This example features the key elements of identity certification: information, documentation, and examination.

Identity claims can be either explicit or implicit. An example of an explicit identity claim is someone stating their name in response to "who are you?" or the swiping of an ATM card. An example of an implicit claim is driving a car (implying you have a license) or purchasing alcohol at a store or bar (implying you are of legal age to purchase alcohol). According to Downes, an identity claim can be supported by either assertions or tokens. An assertion is typically a statement such as "I am John Doe," while a token is a physical object such as a driver's license. Downes offers a definition of "identification" as "the act of claiming an identity, where an identity is a set of one or more signs signifying a distinct entity."[12]

[12] Stephen Downes, "Authentication and Identification." International Journal of Instructional Technology and Distance Learning. Oct 2005 at 2.

Identity certification is not just about claiming one's own identity. It is also about claiming an identity in order to gain access to a particular resource.[13] The idea of access in the process of identity certification is valuable as it helps pinpoint the context in which identity is often presented. In a broad sense, the resource could be the legal ability to drive a car, have access to money in a bank account, or permission to enter a particular facility, space, or country.

Following the claim of identity comes the step of authentication or verification of the identity. Authentication can be regarded as "the act of verifying the identity, where verification consists of establishing to the satisfaction of the verifier, that the sign signifies the entity."[14] Three common categories of authenticators relate to "what one knows," "what one has," and "who one is." "What one knows" is usually a password, or the answer to a personal question. "What one has" consists of physical documents or items, such as a key, driver's license, passport, or data chip. "Who one is" refers to biometric characteristics, which can be checked manually by comparing the photograph on an identification document to the presenter, or electronically with systems that compare a feature scan against a central databank.

Identity authentication is largely a matter of trust. Landahl argues that identity authentication involves asking "how certain are we that a person is who they say they are?"[15] This certainty will depend on the procedures used to create the identity document. The more certain people are that the token cannot be forged, the more likely they are to

[13] Doug Gale, "What's in a Name?" *T.H.E. Journal, 33* (11), June 2006, at 22–24.
[14] Stephen Downes, "Authentication and Identification." International Journal of Instructional Technology and Distance Learning. Oct 2005 at 2–3.
[15] Mark Landahl, "Identity Crisis: Defining the problem and framing a solution for terrorism incident response." *Homeland Security Affairs, 3* (3) Sept 2007, at 2–3.

trust the verification of the identity claim. The importance of trust to the identity certification process cannot be overstated; it is crucial.

Information used for identity certification can also be classified as "non-biometric" or "biometric." Both categories work interdependently in identity certification processes.

### 3.1 Non-Biometric Identifiers

Non-biometric identifiers are characteristics that are not universal, distinct, permanent, and collectible.[16] The most common example is a person's name. When asked "who are you?" most people respond with their name. It is the principal piece of information on most identification cards. Other non-biometric identifiers include place of birth, date of birth, gender/sex, age, parents' names, criminal record status, citizenship, or identification codes or numbers. Much of the visible information on identity cards consists of non-biometric identifiers.

Currently very little identity certification is done using a single non-biometric identifier. As names can be shared or reproduced, additional information is typically required to establish a unique identity. The modern requirement for "two factor authentication" is exemplified by the act of swiping an ATM card (identity claim), and entering a Personal Identification Number (PIN) code (verifying that the presenter of the card is the owner of the card, and has a right to the resources).[17]

[16] There is no standard definition of "non-biometric information" in the literature. Most often the term "non-biometric information" is used in contrast to "biometric information." The definition here is an adaptation of standard definitions of biometric information.
[17] Doug Gale, "What's in a Name?" *T.H.E. Journal, 33* (11), June 2006, at 22–24.

Two-factor authentication can also include the use of biometric identifiers. There is a higher level of trust when a physical characteristic of a person is linked to a claimed identity. For example, it is more difficult for a person to replicate or fabricate another person's fingerprint or facial image than it is their date of birth or postal code.

### 3.2 Biometric Identifiers

Biometric characteristics are physiological or behavioural characteristics that can be used to authenticate an identity. Any characteristic can be useful biometric information so long as it is (relatively)[18] universal, (relatively) permanent, distinct, and collectible.[19] The three functions of biometrics are:

1. Verification/authentication of an identity;
2. Identification/confirmation—"is this person in the database?";
3. Screening—"is this a wanted person?"[20]

The current and potential uses of biometrics are varied as indicated by the following table.

Table 1. Examples of where biometric systems are used.

| **High Government Use** | **Low Government Use** | **Private Sector Use** |
|---|---|---|
| Law Enforcement<br>Prison Management<br>Military & National Security Community | Border Control & Immigration Checks<br>Entitlement Programs<br>Licensing<br>National Identity Card & Voter Registration | Banking and Financial Services<br>Personnel Management Access Control<br>Information System Management |

Source: John D. Woodward Jr., "Biometrics: Identifying Law and Policy Concerns." In Anil K. Jain et al. eds. *Biometrics: Personal Identification in a Networked Society*. New York: Springer, 2006.

[18] Anil K. Jain et al., *Handbook of Fingerprint Recognition*. New York: Springer, 2003, at 26.
[19] Anil K. Jain et al., "An Introduction to Biometric Recognition." *IEEE Transaction on Circuits and Systems for Video Technology, 14* (1) Jan. 2004, at 1–2.
[20] Anil K. Jain, Arun Ross, and Sharath Pankanti, "Biometrics: A tool for information seeking." *IEEE Transaction on Information Forensics and Security, 1* (2) June 2006, at 130.

The user must enrol in the biometric system by submitting a sample of their feature (fingerprints, photo, etc.). These images are then processed into numerical format and entered into a database. For identity authentication, biometric systems operate in either one-to-one or one-to-many modes.

One-to-one refers to matching an identity claim against one template. Most commercial applications of fingerprint identity certification operate this way. Users first enrol their sample in the device (such as a laptop, data stick, or cell phone). To access the device, users scan their fingerprint. The fingerprint is then compared to the template in the system.

One-to-many refers to comparing the claimed identity against a larger database. For example, when facial scans are taken in a crowd and compared against people on a "watch list" or central databank.

### 3.2.1 Facial Recognition[21]

Facial geometry is one of the primary methods for recognizing people. In its simplest form, facial geometry consists visually of matching a face to a photograph. Methods have evolved to incorporate digital photographs, automated systems, and biometric processing technologies. The format of the image captured depends on the system. The image can be 2-D, 3-D, colour, black and white, infrared, or a combination.[22] The two most popular approaches to automatic facial recognition use the location and

[21] For a comparative table of the general properties of most frequently used biometric characteristics, see Appendix A.
[22] John J. Weng and Daniel L. Swets, "Face Rocognition," In Anil K. Jain et al. eds., *Biometrics: Personal Identification in a Networked Society*, New York: Springer, 2006, at 43–65.

shape of facial attributes – such as eyes, ears, lips and their spatial relationships – or use an overall analysis of the face.[23]

Facial biometrics is a non-intrusive and familiar method of identity certification, and has become widespread in surveillance efforts. Facial recognition is employed in Britain's vast surveillance closed-circuit television (CCTV) network, as well as at large-scale sporting events, airports, and public crowds. In some U.S. states, facial recognition is used in casinos to identify high-risk or banned individuals. Mr. Payroll Corp in the U.S. has also begun using facial recognition for its cheque cashing system.[24]

Governments have also been increasing their use of this technology. One example is the U.S. Visa Waiver program, which now requires a secure identity document containing facial biometric data.[25] Canada has begun to move towards facial recognition systems in federally issued identity documents and provincially issued enhanced driver's licenses. Amendments in 2004 to the *Canadian Passport Order*[26] authorized Passport Canada to convert submitted information into digital biometric form to be included in the passport, as well as to convert an applicant's photograph into a biometric template for the purpose of identity verification.[27] Once fully operational, the system will use the biometric information to "perform identification and verification tasks, and would compare applicants' facial images to those on a watch list compiled from a variety of

[23] Anil K. Jain, Arun Ross, and Sharath Pankanti, "Biometrics: A tool for information seeking." IEEE Transactions on Information Forensics and Security, 1 (2), June 2006, at 126.
[24] Alex Pentland and Tanzeem Choudhury, "Face Recognition for Smart Environments." *Computer, 33* (2) Feb. 2000, 50–55, at 52.
[25] VISA Waiver Program, United States Department of State: http://travel.state.gov/visa/temp/without/without_1990.html.
[26] *Canadian Passport Order* (SI-81-86).
[27] *Order Amending the Canadian Passport Order*, P.C. 2004-951, 1 September 2004.

sources."[28] British Columbia, Alberta, Quebec, and Ontario have begun developing driver licenses with facial biometric information to meet both Canadian and U.S. border crossing requirements.[29]

### 3.2.2 Hand Geometry

Hand geometry involves taking a number of measurements of the user's hand. These can include hand shape, size of the palm, and the lengths and widths of fingers. Hand geometry is not known to be very distinctive.[30] Because of this limitation, it is only suitable for one-to-one matching. However, there are several advantages of systems that use hand geometry recognition, such as medium cost, fast computation, low template size, ease of use, and low maintenance.[31]

Hand geometry recognition is based on a photograph of the top, side, and/or bottom of the hand. The hand is placed on a sensor, which activates a camera and then captures the image. The image is processed by taking the required measurements of the hand and then processing these measurements into biometric data.

Hand geometry is currently used in a variety of settings. University dorms and other buildings use it for student access. The 1996 Olympic Games also used hand geometry to control access to the athlete's village. Walt Disney World used it to identify

[28] Lalita Acharya, "Biometrics and Government." Government of Canada: Parliamentary Information and Research Service, Sept. 2006, at 10–11.
[29] For a timeline of events leading up to the provincial creations of enhanced identifications, and which provinces have begun implementing them, see Canada Border Services Agency, "Documents to Travel to the United States: Chronology." Nov. 6, 2008: http://www.cbsa-asfc.gc.ca/whti-ivho/chron-eng.html.
[30] Anil K. Jain, Arun Ross, and Sharath Pankanti, "Biometrics: A tool for information seeking." *IEEE Transactions on Information Forensics and Security, 1* (2) June 2006, at 126.
[31] Rand Sanchez-Reillo and Ana Gonzalex-Marcos, "Access Control System with Hand Geometry Verification and Smart Cards." *IEEE AES Systems Magazine*, Feb. 2000, at 46.

valid season ticket holders. It is also used in workplaces to clock employee attendance and time worked.[32]

### 3.2.3 Fingerprinting

Fingerprints are a ubiquitous form of biometric information used primarily for law enforcement purposes. Fingerprints, however, are increasingly being used for commercial applications that employ identification systems such as laptops, desktops, cellular phones, and data sticks.

The strength of fingerprint biometric information comes from a longstanding belief that no two fingerprints are identical. However, fingerprints can replicate in two individuals, albeit with chances estimated around 1 in 64 billion.[33] The uniqueness of fingerprints may be compromised when the image scanner takes only a portion of the distinguishing information, instead of the entire print. Modern biometric systems have moved towards smaller print sizes in order to save data space, possibly affecting the distinctiveness of the fingerprint and/or the enrolment rates.[34] Despite this, fingerprints remain a high-grade biometric characteristic due to their unique characteristics. Identity certification methods that use fingerprint biometric technology are considered strong compared to other biometric systems.[35]

---

[32] Anil K. Jain, Arun Ross, and Sharath Pankanti, "Biometrics: A tool for information seeking." *IEEE Transactions on Information Forensics and Security, 1* (2) June 2006. at 141.
[33] "Individual Biometrics." National Center for State Courts. 2002: http://ctl.ncsc.dni.us/biomet%20web/BMFingerprint.html.
[34] Anil R. Jain et al., *Handbook of Fingerprint Recognition*. New York: Springer, 2003, at 26.
[35] For detailed technical descriptions see Anil K. Jain et al., *Handbook of Fingerprint Recognition*. New York: Springer, 2003.

Governments largely use fingerprinting in law enforcement. For example, the US-VISIT program collects, maintains, and shares information such as digital finger scans to screen incomers against watch lists. The FBI maintains the world's largest biometric database (the Integrated Automated Fingerprint Identification System), storing the fingerprint data of around 47 million subjects.[36]

Canadian law enforcement has also moved towards an Automated Fingerprint Identification System (AFIS). The "Real Time Identification Project" is an RCMP project aimed at modernizing its fingerprint processing. The goal is to move away from paper- and manual-based applications toward systems that promote "rapid fingerprint identification" and "the immediate update of the associated criminal." The project aims to facilitate data sharing with other national and international partners.[37]

### 3.2.4 Iris Recognition

The iris has become an increasingly salient biometric characteristic for identity certification. The iris contains distinct patterns that make it analogous to fingerprints, in that patterns differ enormously between individuals. Moreover, up to a third of the iris can be damaged before its usability is compromised.[38]

The patterns of the iris are captured and processed into biometric data, or an "iris code."[39] Iris recognition is used for some computer or network logins in high security

[36] Lalita Acharya, "Biometrics and Government." Government of Canada: Parliamentary Information and Research Service, Sept 2006, at 10–11.
[37] "Real Time Identification Project." Royal Canadian Mounted Police. http://www.rcmp-grc.gc.ca/rtid/index_e.htm.
[38] John Daugman, "How Iris Recognition Works." *IEEE Transactions on Circuits and Systems for Video Technology, 14* (1) Jan. 2004.
[39] Michael Negin et al., "An Iris Biometric System for Public and Personal Use." *Computer, 33* (2) Feb. 2000, at 73.

environments. It is also used by the U.S. military in Iraq and Afghanistan for screening employees, controlling site access, and monitoring inmates and suspected terrorists.[40]

### 3.2.5 Handwritten Signature

The signature is a behavioural biometric characteristic. Signatures are highly variable and hard to verify automatically. Verification systems capture the image either during the writing process or after. Strategies used to capture the image during the writing process involve a video recording of the user writing with pen on paper, or the use of an electronic pen on a sensor designed to record velocity, acceleration, pressure, and/or pen inclination. Manual inspection, however, is still more common.[41]

### 3.2.6 Other Biometric Methods[42]

Audio-visual biometric systems operate by linking static video frames of the face or certain parts of the face and/or video sequences of the face or mouth area with a voice capture method. Strong correlations have been shown between face motion, vocal tract shape, and speech acoustics. Audio-visual biometric systems can operate in low security and highly user-friendly applications, such as desktop computer access. Audio-visual-based biometric systems are successful in a variety of scenarios, including those focused on security.[43]

---

[40] Dawn S. Onley. "Biometrics on the front line." *Government Computer News*. Apr. 16, 2008. http://www.gnc.com/print/23_23/26930-1.html?page=1.
[41] See S. Impedovo and G. Pirlo, "Verification of Handwritten Signature: An Overview." 14th International Conference on Image Analysis and Processing, 2007.
[42] There are scores of biometric characteristics being researched and implemented in new technology. Some not mentioned here but possible to appear in the future: retina, gait, odour, vein, thermal, and reflex.
[43] Petar S. Aleksic and K. Katsaggelos Aggelos, "Audio-Visual Biometrics." Proceedings of the IEEE, 94 (11) Nov. 2006, at 2026–2028.

DNA is a highly distinctive feature. DNA has shown strong usefulness in forensic applications, such as parental identification, but is considered highly intrusive and is often associated with the criminal justice process. Technological improvements would need to be made in order for DNA to be used for identity certification, as it cannot currently be typed sufficiently quickly to be commercially viable.[44]

### 3.3 Limitations of Biometric Methods

Based on the above review, there are two important limitations in using biometric identifiers. One limitation occurs when a method fails to be accessible. The second limitation relates to discretionary decisions made through manual inspection.

#### 3.3.1 Accessibility

From a human rights perspective, accessibility refers to the notion that an intended user should be able to make use of something – for example, a fingerprint biometric system – without confronting barriers based on race, national or ethnic origin, colour, religion, age, sex, sexual orientation, marital status, family status, disability or a pardoned conviction. Based on the review, an identity certification method may be inaccessible for a variety of reasons.

A biometric system may be inaccessible at enrolment where the technology fails to enrol the physiological or behavioural characteristic because a person does not have the required biometric identifier. As a result, an applicant may be refused an identification document based on their disability (ie. missing fingers, hands, irises) if the document depends only on the particular biometric that cannot be given.

[44] See Gary Roethenbauch, "Biometrics Explained." International Committee for Information Technology Standards, Sept. 2005.

Alternatively, a biometric system may be inaccessible if the user possess a feature that cannot be read by the system. Fingerprints, for example, can become inadequate for even advanced systems. Despite the ubiquity of fingerprint identification systems, there is a small percentage of the population that cannot be enrolled. This is due to the wearing down of ridges and/or drying of the skin because of age, genetic factors, environmental conditions, working conditions, or physical damage to the fingertip.[45] Individuals who experience tremors or other motor related difficulties may also find it problematic to enrol. Failures to enrol also tend to be higher for Black compared to White subjects and for women compared to men.[46]

Even if individuals successfully enrol in a given system, biometric systems can remain inaccessible by the extent to which they generate inaccurate results.[47] A U.K. study on biometrics, for example, identified a higher accuracy rate for Asian compared to Caucasian subjects when using facial recognition methods. Accuracy rates were also better for older individuals and for men.[48] Some technologies, however, are better than others by virtue of the type of characteristic being sampled. The accuracy rates for technologies such as iris recognition are very high.[49]

### 3.3.2 Discretionary decisions based on manual inspection

The second limitation arises when a person's identity becomes the object of manual inspection. As referred above, this is commonly done with handwritten

[45] Anil K. Jain, Arun Ross, and Sharath Pankanti, "Biometrics: A tool for information seeking." *IEEE Transactions on Information Forensics and Security, 1* (2) June 2006, at 126.
[46] UK Passport Service. "UKPS Biometrics enrollment trial report." May 2005.
[47] Accuracy rates refer to the frequency of false positives and false negatives. A false negative occurs when a system fails to identify someone as the person he/she claims to be. A false positive occurs when a system identifies someone as someone else.
[48] UK Passport Service. "UKPS Biometrics enrollment trial report." May 2005.
[49] John Daugman, "How Iris Recognition Works." *IEEE Transactions on Circuits and Systems for Video Technology, 14* (1) Jan. 2004.

signatures. Though manual inspection may be more accurate than certain biometric technologies, there is an inherent potential that a person's identity may be assessed based on individual biases and prejudices, the consequences of which may lead to racial or other forms of discriminatory profiling.[50]

### 3.3.3 Means of mitigating biometric limitations

Testing and data collection are two techniques that can be used to measure, identify and deal with potentially negative discriminatory effects generated by a given technology on a group of individuals. For example, the image size of the fingerprint used in an Automated Fingerprint Identification System (AFIS) can affect the failure to enrol rates – the smaller the size, the higher the number of users who will be unable to enrol based on the properties of their fingertips. Such was the case with the British national identification card. The system had difficulty enrolling people over the age of 75. It was suggested that higher-grade fingerprints be obtained by increasing the image size.[51] Testing the technology on a representative sample of intended users to see whether a particular group of people is excluded, and then developing the technology in response to the results, can encourage greater participation and accuracy.

Data collection is not only important during the testing stage of a given technology, but also during its implementation especially where manual inspection or verification is practiced. The type of data collected should include human rights-based

[50] Joint Canadian Human Rights Commission and Canadian Race Relations Foundation Position on the Importance of Data Collection in Addressing Profiling. http://www.chrc-ccdp.ca/research_program_recherche/profiling_profilage/page9-en.asp

[51] Ian Drury, "ID cards could be derailed by pensioners as finger prints of over-75s are hard to scan." *The Daily Mail*, Aug. 15, 2008: http://www.dailymail.co.uk/news/article-1045659/ID-cards-derailed-pensioners-finger-prints-75s-hard-scan.html.

data[52] where appropriate. This includes information on a person's race, national or ethnic origin, colour, religion, age, sex, disability, and/or pardoned conviction where appropriate. Whenever a discretionary decision is made by an officer in verifying a person's identity, recording human rights-based data and the type of decision rendered can track whether stereotypes or biases are entering into the decision making process.

## 4. The Use of Non-Biometric and Biometric Methods in Identity Documents

Modern societies have required that citizens accumulate identity documents for many reasons. The variety of types and purposes of these documents has encouraged researchers to categorize them into two main categories: "breeder documents" and "secondary identity documents."[53] "Breeder documents" refer to identity documents confirming birth, such as birth, baptismal, and adoption certificates. "Secondary identity documents" refer to documents required for particular identity certification purposes, such as passports, visas, driver's licenses and citizenship cards. Breeder documents are needed to obtain any secondary identity documents that relate to identity certification.

A weakness of the current scheme of issuing secondary identity documents is the reliance on breeder documents as primary identity documents since one need only obtain fraudulent breeder documents in order to obtain fraudulent secondary identity documents.

---

[52] For more information, please refer to the *Joint Canadian Human Rights Commission/Canadian Race Relations Foundation Position on the Importance of Data Collection in Addressing Profiling*. http://www.chrc-ccdp.ca/research_program_recherche/profiling_profilage/page9-en.asp

[53] See Alane Kochems and Laura Keith. "Successfully Securing Identity Documents: A Primer on Preventive Technologies and ID Theft." *Heritage Foundation Backgrounder*. No. 1946, June 27, 2006.

To mitigate this weakness, biometric systems are used to strengthen secondary identity documents by establishing another layer of uniqueness to the identity document.[54]

Identity certification is dependent on the uniqueness of the information provided. Birth dates are used to distinguish between people with the same name. The introduction of photographs onto the identity document is an early example of the use of a biometric characteristic in establishing a stronger link between the token and the identity claimed. The addition of other biometric characteristics to identity documents augments the trust necessary for secondary documents to be considered valid tokens.

Many government-issued documents that allow Canadians or individuals residing in Canada the ability to travel require various non-biometric and biometric identifiers. The following review of the Passport, the Canadian Permanent Resident Card, CANPASS AIR and NEXUS illustrate how identity certification methods are used.

### 4.1 Passport, Canadian Permanent Resident Card, CANPASS AIR, NEXUS

"The passport has become the key signifier of identity and an elemental requirement of full participation in the global marketplace."[55] Under the *Passport Order*, Passport Canada has the authority to grant or refuse a passport. Refusal may be based on providing false information in the passport application process, having been charged with a serious offence, being currently imprisoned, being forbidden to leave Canada, being forbidden to possess a passport, or having been convicted of a passport related offence in

[54] Anil K. Jain, Arun Ross, and Sharath Pankanti, "Biometrics: A tool for information seeking." *IEEE Transactions on Information Forensics and Security, 1* (2) June 2006, at 140.
[55] "Backgrounder: Refusal or Revocation of Passports." Passport Canada: http://www.ppt.gc.ca/articles/20080213a.aspx?lang=eng.

Canada or abroad. Revocation may occur when a person uses the passport to commit a serious offence in Canada or abroad, permits another person to use their passport, or has obtained the passport by means of false or misleading information.[56]

The primary requirement for a Canadian passport is Canadian citizenship (ie. old passport, birth certificate, certificate of citizenship). Other requirements include documents to support the applicant's identity. These supporting documents may be a driver's license, health card, certificate of Indian status, other federal/provincial/municipal identification or employee cards, old passport, U.S. permanent residency card, and/or old age security card.

The Canadian Permanent Resident Card is an identity document that certifies a person's official status upon entry into Canada and gives access to certain government services and programs.[57] The cards were introduced in 2002 in line with the *Action Plan for Creating a Secure and Smart Border*. All new permanent residents would immediately receive a card, with all existing permanent residents having to apply for one. To be eligible, applicants must be permanent residents of Canada, and be physically present in Canada. Applicants cannot be under an effective removal order, or be convicted of an offence related to misuse of a Permanent Resident Card.

[56] "Backgrounder:" Refusal or Revocation of Passports." Passport Canada: http://www.ppt.gc.ca/articles/20080213a.aspx?lang=eng.
[57] "Permanent Resident Card." Citizenship and Immigration Canada: http://www.cic.gc.ca/EnGLIsh/information/pr-card/index.asp

CANPASS is a solely Canadian operated program. The CANPASS Air program[58] allows "pre-determined low-risk" users to return to Canada more expediently by bypassing custom and immigration checks in Canadian airports, land, and water crossings.[59] The program began in 2003, and is now offered in most major airports across the country. The security check includes a review of the applicant's criminal, customs, and immigration status in order to determine their risk level. These checks are re-done annually.

Implemented in 2004, NEXUS is a joint Canada–U.S. run program currently operating at select Canadian and American airports. The goal of the program is to facilitate the rapid processing of low-risk travellers across the border. This process includes the gathering and maintaining of data on travellers before they cross the border. The NEXUS card represents the most rigorous border crossing identification in Canada. The eligibility requirements are that a person must:

- Be a citizen or permanent resident of Canada or the U.S.
- Be admissible to Canada or the U.S. under immigration laws
- Provide true and accurate information
- Meet all other requirements of NEXUS (application form, security check)
- Have no recorded violations of customs, immigration, or agriculture laws

[58] There is also CANPASS Highway, CANPASS Corporate Aircraft, CANPASS Private Aircraft, and CANPASS Boat. CANPASS Air is the most complex and progressive, and will therefore serve as the example for discussion.
[59] CANPASS Air. Canada Border Services Agency: http://www.cbsa-asfc.gc.ca/prog/canpass/canpassair-eng.html.

A person will not be eligible if convicted of a serious criminal offence in any country for which a pardon has not been granted.[60]

The passport, CANPASS Air, and NEXUS programs are voluntary systems. Canadians are not required to obtain any of these documents. However, in order to travel, Canadians' require at least one of these documents to leave and re-enter the country. The Canadian Permanent Resident Card is not a voluntary system. As mentioned, all new permanent residents will receive a card. Existing permanent residents are not required to obtain the card, but the card may be required to access certain services within Canada and for travel abroad.

### 4.2 Requirements of non-biometric identifiers

The passport, Canadian Permanent Resident Card, CANPASS Air, and NEXUS all request similar forms of non-biometric information. Table 2 outlines the information required for each document. The primary pieces of information are name, date of birth, sex/gender, and address. All applications require an employment and residence history, although they vary as to whether they require two or five years. An applicant has the option of having the place of birth not appear on the document, but they are still required to provide this information on the application form.

Table 2. Non-biometric information required to be eligible to receive a passport, Canadian Permanent Resident Card, CANPASS Air, and NEXUS.

| Non-biometric Information | Passport | Canadian Permanent Resident Card | CANPASS Air | NEXUS |
|---|---|---|---|---|

[60] "Join NEXUS." Canada Border Services Agency, Jan. 11, 2008. http://www.cbsa-asfc.gc.ca/prog/nexus/elig-admis-eng.html.

| | | | | |
|---|---|---|---|---|
| **First, Middle, Last Names** | X | X | X | X |
| **Birth Date** | X | X | X | X |
| **Marital Status** | X | X | | |
| **Place of Birth** | X (can apply to have it removed from passport) | | | |
| **Sex/Gender** | X | X | X | X |
| **Eye Colour** | X | X | | |
| **Hair Colour** | X | | | |
| **Height** | X | X | | |
| **Weight** | X | | | |
| **Telephone Number** | X | X | | |
| **Guarantor declaration** | X | | | |
| **Address** | X | X | X | X |
| **Address for last two years** | X | | | |
| **Address for last five years** | | X | X | X |
| **Employment history for last two years** | X | | | |
| **Employment history for last five years** | | X | X | X |
| **Educational history for last five years** | | X | | |
| **References** | X | | | |
| **Emergency Contact** | X | | | |

| | | | | |
|---|---|---|---|---|
| **Year of Marriage if requesting spousal surname** | X | | | |
| **Travelled or lived outside of Canada in last five years?** | | X | | |
| **Canadian Citizenship** | X | | X | X |
| **Other** | | Date you became permanent resident | | Member of other border crossing programs? |

### 4.3 Requirements for the use of biometric identifiers

The facial photograph is required for the passport, Canadian Permanent Resident Card, CANPASS Air and NEXUS documents. The CANPASS Air and NEXUS also require an iris scan as their principal biometric characteristic. The proposal for the creation of the Canadian Permanent Resident Card in the *Action Plan* included the use of biometrics; however, this had not been implemented at the time of writing.[61] There are standard requirements for photos: neutral expression, light background, and nothing obstructing the face. These requirements ensure the ability to use the photo in biometric-based facial recognition techniques.

Table 3. Biometric information required for the passport, Canadian Permanent Resident Card, CANPASS Air, and NEXUS.

| Biometric Information | Passport | Canadian Permanent Resident Card | CANPASS Air | NEXUS |
|---|---|---|---|---|
| **Signature** | X | X | X | X |

[61] A pilot project has been undertaken to determine the effectiveness of the system as it relates to non-citizen travellers. A feature of this project is the use of a photograph and fingerprints to certify identity, with positive results reported so far. Fingerprints are not currently a requirement for obtaining the Permanent Resident Card so it is not included on the chart. "Frequently Asked Questions: Biometrics Field Trial." Citizenship and Immigration Canada, June 12, 2008: http://www.cic.gc.ca/english/inFORMation/faq/biometrics/index.asp.

| | | | | |
|---|---|---|---|---|
| **Photograph** | X | X | X | X |
| **Fingerprint** | | | | X |
| **Iris** | | | X | X |

### 4.4 Human rights legal issues that have arisen from the use of non-biometric identifiers

There has been no legal issue so far regarding the use of non-biometric information. The most relevant case is *Veffer v. Canada*.[62] Mr. Veffer had entered "Jerusalem, Israel" as his place of birth on his application for a passport. Passport Canada has a policy of listing "Jerusalem" as a stateless city, as recognized by the United Nations, and listed it as such on his passport. Mr. Veffer then filed a suit against Passport Canada claiming this violated his rights to equality and religion under the *Charter*. The Federal Court of Appeal rejected his arguments, finding that he had the option of leaving the field blank on his passport as per Passport Canada's exemption policy or listing "Jerusalem." As a result, his rights were not unreasonably infringed because of the options provided to him. Passport Canada does inform applicants that certain countries may not accept a passport if place of birth is not visibly listed, and that this must be taken into consideration when applying for the exemption to have the field left blank on a passport.

### 4.5 Human rights legal issues that have arisen from the use of biometric identifiers

Facial requirements for provincial driver's licenses have faced human rights challenges based on religious objections, particularly related to the use of a photograph.

[62] *Veffer v. Canada (Minister of Foreign Affairs).* 2007 FCA 247. Leave to appeal denied by the Supreme Court of Canada, 2007 WL 4926336 (S.C.C.), [2007] S.C.C.A. No. 457.

In *Bothwell v. Ontario*,[63] Mr. Bothwell objected to having his photograph taken and stored in a computer database. He subsequently applied for a religious exemption offered by the province, and was denied. Mr. Bothwell then filed a case against the Ontario government claiming it had discriminated against his religious beliefs. The court found Mr. Bothwell's objections not to be sincerely based in religious belief, and found in favour of the government. The court did not address the question of whether the requirement infringed his freedom of religion.

The courts in *Hutterian Brethren v. Alberta*[64] did address whether the photograph requirement infringed the religious beliefs of the Hutterite faith. The Hutterites objected to having their photographs taken under any circumstance. They had been using an exemption under the provincial *Traffic and Safety Act*[65] (*TSA*), which permitted applicants to obtain a license without a photograph if they had a sincerely held religious objection. There were about 450 of these "Condition Code G" licenses, 56 percent of which were held by Hutterian Brethren. The exemption was removed when the legislation was updated in 2003 to recognize Alberta's attempts at developing an "enhanced driver's license" and databank featuring biometric facial information. The province did offer two alternatives to the new standard licence, but both still involved being photographed. The Hutterian Brethren proposed instead that no photograph be taken and that non-photo driver's licences be issued to them marked "Not to be used for identification purposes."

---

[63] *Bothwell v. Ontario (Minister of Transportation).* [2005] O.J. No. 189.
[64] *Hutterian Brethren of Wilson Colony v. Alberta.* 2007 ABC 160, 49 M.V.R. (5th) 45. Leave to Appeal at Supreme Court of Canada granted in, 2007 WL 4227549 (S.C.C.)
[65] *Traffic Safety Act*, R.S.A. 2000, c. T-6 (*TSA*)

The trial judge and the Court of Appeal found that, by removing the exemption that the Hutterian Brethren had used for the past thirty years and not offering anything in its place, the province had unreasonably infringed upon their freedom of religion under the *Charter*. The majority at appeal found that the provincial *TSA* was primarily concerned with highway safety and license provision, and therefore could not be said to have national security or border crossing as a focused mandate. The majority decision qualified its response that "in some circumstances, the desire of a government to harmonize its security standards with other jurisdictions may be of sufficient importance to warrant infringement of a right protected by the *Charter*."[66] The dissenting judge criticized the majority's reading of the *TSA* as being too narrow. The dissent found the *TSA* necessarily had to encompass concerns of national security and international security, since driver's licenses are being used as border documents.[67]

The case was appealed to the Supreme Court of Canada, where it proceeded on the basis that the mandatory photo requirement infringed the right to freedom of religion, and focused on whether that infringement could be justified under section 1 of the *Charter*. The majority found in favour of the province, stating that Alberta's attempts to make the driver's licence a more secure document outweighed the religious freedom of the Hutterian Brethren. Summarizing paragraphs 39, 42, and 45, the Court stated that

> Regulations are measures "prescribed by law" under s.1, and the objective of the impugned regulation of maintaining the integrity of the driver's licensing system in a way that minimizes the risk of identity theft is clearly a goal of pressing and substantial importance, capable of justifying limits on rights. The universal photo requirement permits the system to ensure that each licence in the system is connected to a single individual, and that no individual has more than one licence.

[66] *Hutterian Brethren of Wilson Colony v. Alberta*. 2007 ABC 160, 49 M.V.R. (5th) 45, at para 31.
[67] See especially paras 88–97.

> The Province was entitled to pass regulations dealing not only with the primary matter of highway safety, but also with collateral problems associated with the licensing system.[68]

Another case involves a hand-geometry-based biometric system that came under challenge in an Ontario labour grievance case against the 407 ETR Concession Company.[69] The employer had begun installing a right-handed scanning biometrics system throughout the workplace to control employee access to various buildings, as well as clocking attendance and time worked. Several employees of the Pentecostal faith filed the initial grievance but most dropped the grievance after it was proposed that they use their left hand instead of their right. Nonetheless, three employees still objected.[70] The Arbitrator found that "the biometric scanner discriminates against the grievors on grounds of their creed,"[71] and that the employer had not accommodated these three employees to the point of undue hardship. While the union and the grievors proposed an alternate system using a swipe card and password, the employer simply terminated the employees.[72] In response, the Arbitrator offered other possible options, but ultimately left the decision to the union and the employer to resolve.[73]

## 5. The Impact of Biometrics on Human Rights: Two Key Principles

Two key human rights principles emerge from the review. The first principle is that service providers[74] have a duty to accommodate individuals who belong to one of the

---

[68] *Alberta v. Hutterian Brethren of Wilson Colony*, 2009 SCC 37
[69] *407 ETR Concession Co. v. CAW-Canada Local 414.* [2007] L.V.I. 3701-1.
[70] Pentecostal faith permits a large range of individual discretion so the beliefs of one Pentecostal may not entirely reflect the beliefs of another. Thus, the court found that their beliefs were sincere, even though they differed from their co-workers. Because of this, the Board found "creed" to be a much more appropriate ground than "religion." *407 ETR Concession Co. V. CAW-Canada Local 414.* [2007] L.V.I. 3701-1. para 120.
[71] *407 ETR Concession Co. v. CAW-Canada Local 414.* [2007] L.V.I. 3701-1. para 179.
[72] *407 ETR Concession Co. v. CAW-Canada Local 414.* [2007] L.V.I. 3701-1. para 179.
[73] *407 ETR Concession Co. v. CAW-Canada Local 414.* [2007] L.V.I. 3701-1. para 181.
[74] The duty to accommodate applies both to service providers and employers.

groups protected under the *CHRA* short of undue hardship. The second is that service providers can implement a measure that excludes members of a protected group if it can be justified.

### 5.1 The Duty to Accommodate

The Supreme Court of Canada has indicated that while human rights principles acknowledge "that not every barrier can be eliminated,"[75] employers and service providers alike have a duty to prevent new barriers from arising. Measures should be developed in such a way as to be as inclusive as possible without discriminating against individuals based on a prohibited ground. *Ad hoc* accommodations should only be considered in unforeseen situations.[76] When developing identity documents that employ biometrics, such measures should therefore be developed in a manner that allows the largest number of individuals to participate. Where technological limits exist, alternative and/or supplemental metrics ought to be considered.

Multi-modal systems inherently accommodate individuals who may lack a particular characteristic or have a characteristic that cannot be initially read. It is recommended that for security sensitive applications, multi-modal systems that crosscheck more than one feature be used.[77] One example of a multi-modal system is that used by the American government for federal employees: "While the Personal Identity Certifier (PIC) card stores both the fingerprint and facial-scan biometrics for each enrolled federal employee or contractor, it primarily uses fingerprint biometrics. Digital

---

[75] *Council of Canadians with Disabilities v. VIA Rail Canada Inc.,* [2007] 1 S.C.R. 650, 2007 SCC 15. para 186.
[76] *Council of Canadians with Disabilities v. VIA Rail Canada Inc.,* [2007] 1 S.C.R. 650, 2007 SCC 15. para 175.
[77] Anil K. Jain et al., *Handbook of Fingerprint Recognition*, New York: Springer, 2003, at 37.

facial-image scan is used when it is not possible for a federal employee or contractor to provide fingerprints or if there is an anomaly."[78]

Multi-modal systems can also be used to accommodate individuals should the individual raise a particular objection. In the grievance case against the 407 ETR Concession Company, for example, the Arbiter suggested that the employer use a multi-modal approach by not only offering a hand-geometry-based biometric but also a swipe card and password system.

An alternative form of built-in accommodation is to have policies and/or practices in place that allow for limited exceptions. Though not reviewed in the first half of the report, the following example illustrates how a policy can accommodate religious observance without undermining the effectiveness of the technology.

In 2007, three Sikh children were denied passports because of their photos. In their photos, they were all wearing headpieces as prescribed by their faith. None of their headpieces obstructed their faces, conforming to Passport Canada's policy that states, "so long as we can clearly see their facial traits and they provide a written request," headpieces are permitted. Once the story was featured in the media, Passport Canada issued passports and apologies to the children and their parents. Passport Canada stated the denial was a mistake, and the officers involved received training to help prevent similar policy misapplications.[79] In this example, a policy to accommodate religious practice was developed beforehand in order to allow individuals access to a passport

[78] Babita Gupta, "Biometrics: Enhancing Security in Organizations." IBM Center for the Business of Government, 2008, p. 27.
[79] "Passport Canada says Sikh photos rejected by mistake." CBC News. Aug. 17, 2007: http://www.cbc.ca/canada/british-columbia/story/2007/08/17/bc-passportcanada.html

without infringing on their human rights, without compromising the effectiveness of the biometric technology.

### 5.2 A *Bone Fide* Justification

The courts have recognized that on some occasions, accommodation may not be possible. In such circumstances, an organization must provide an evidence-based justification.

An immediate example is that of the Hutterian Bretheren case. Here the Supreme Court of Canada recognized that goals of a pressing and substantial importance, if demonstrated, may limit the exercise of certain rights. Though the Court decided the case based on a *Charter* section 1 analysis, the concept is similar in human rights legislation. A *bona fide* justification according to human rights law can be argued when an organization can demonstrate that the measure in question has been designed with a particular and legitimate objective in mind; that there is a demonstrated link between the measure and the objective; that the measure is reasonably necessary to accomplish the objective; and that it includes alternative arrangements for those who require accommodation short of undue hardship.

## 6. Conclusion

The purpose of this paper was to explore the ways in which various identity certification methods used in such documents as the Passport and NEXUS could have a human rights impact. Protecting human rights involves anticipating areas of potential differential treatment, and acting to provide flexibility, where possible, in order to

achieve a solution with the least negative impact on the groups protected under the *CHRA*.

A review of identity certification methods has demonstrated that certain limits exist, which may have the potential of affecting a person's human rights in a differentially adverse manner. Depending on how the technology is developed, the method may be inaccessible to an individual or a group of individuals. One way of mitigating such difficulties is by testing the technology on a representative sample of intended users. Monitoring should be done on a continual basis. If the method includes manual inspection, human rights-based data should also be collected to help identify any systemic biases.

The review also demonstrated that accessibility issues related to uni-modal systems can sometimes be addressed through accommodation. As seen in the *407 ETR* case, the affected employees were allowed to use their left hand instead of their right hand in using the hand-geometry-based biometric. However, uni-modal systems may also create and compound existing barriers. Fingerprinting systems, for example, may prove to be inaccessible for individuals of a certain age, profession, or physical condition. Age, working conditions and certain types of disability are three common factors that can reduce the quality of the fingerprint image to the point that the prints are not enrollable. This is why it is recommended that multi-modal systems be employed especially in security environments.

Multi-modal biometric systems offer a degree of accommodation and are promoted as a solution to the limitations of uni-modal systems. One form of multi-modal

system, where two comparably unique characteristics are used, was seen in the U.S. government-employee card system. Where the applicants' fingerprints could not be enrolled, a facial image was used instead. Multi-model systems not only have the capacity to help in protecting human rights but also have the ability to build a stronger and trustworthier security system.

Situations may also arise where users may require an exemption. Policies and practices to accommodate these individuals short of undue hardship should therefore be included as part of the development of any measure. Passport Canada's policy on religious headwear serves as an example. Should there be no reasonable alternative for a given biometric, it is up to the organization employing the biometric to demonstrate that sufficient measures have been taken to explore other less discriminatory ways of achieving the same results short of undue hardship.

Both the *Charter* and the *Canadian Human Rights Act* recognize limits to the exercise of individual rights. The Hutterian Brethren case serves to illustrate a situation where individual rights were limited by public interest objectives of pressing and substantial importance. It is the responsibility of the organization employing the measure to demonstrate that the system was designed in a manner that is consistent with human rights principles.

# APPENDIX A

Table 1. Comparison of Various Biometric Technologies
(H = High, M = Medium, 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 |
| Fingerprint | M | H | H | M | H | M | M |
| Hand geometry | M | M | M | H | M | M | M |
| Iris | H | H | H | M | H | L | L |
| Palm print | M | H | H | M | H | M | M |
| Retina | H | H | M | L | H | L | L |
| Signature | L | L | L | H | L | H | H |

Source: Anil K. Jain et al. “An Introduction to Biometric Recognition.” IEEE Transaction on Circuits and Systems for Video Technology. 14 (1) Jan 2004.

# BIBLIOGRAPHY


**Hansard**

House of Commons. *Subcommittee on Public Safety and National Security of the Standing Committee on Justice, Human Rights, Public Safety and Emergency Preparedness.* 38th Parl., 1er Sess. (June 15, 2005) (Mary Gusella, Chief Commissioner, Canadian Human Rights Commission).

**Reports**

Canada Border Services Agency. "Audit of the NEXUS Application Process: Internal Audit Report." April 2007. http://cbsa-asfc.gc.ca/agency-agence/reports-rapports/ae-ve/2007/nexus-eng.html.

Office of the Auditor General of Canada. "Report of the Auditor General of Canada to the House of Commons: October 2007." http://www.oag-bvg.gc.ca/internet/English/parl_oag_200710_e_23823.html.

**Legislation**

*Canada Human Rights Act* (R.S., 1985, c. H-6).

*Canadian Charter of Human Rights and Freedoms*, Part 1 of the Constitution Act, 1982, being schedule B to the Canada Act 1982 (U.K.), 1982, c. 11.

*Canadian Passport Order* (SI-81-86).

*Highway Traffic Act*, R.S.O. 1990, CHAPTER H.8.

*Order Ammending the Canadian Passport Order*, P.C. 2004-951, 1 September 2004.

*Traffic Safety Act*, R.S.A. 2000, c. T-6.

**Jurisprudence**

*407 ETR Concession Co. v. CAW-Canada Local 414.* [2007] L.V.I. 3701-1.

*About-Al-Rashta v. Canada (Minister of Citizenship and Immigration).* [2001] F.C.J. No. 644., 2001 FCT 344.

*Al-Ghamdi v. Canada (Minister of Foreign Affairs & International Trade.* 2007 FC 559, 64 Imm. L.R. (3d) 67.

*Andryanov v. Canada (Minister of Citizenship and Immigration).* [2007] F.C.J. No. 272, 2007 FC 186.

*Bothwell v. Ontario (Minister of Transportation)*. [2005] O.J. No. 189.

*Canada Safeway Ltd. V. U.F.C.W. Local 401*. [2006] L.V.I. 3607-3, 145 L.A.C. (4th) 1.

*Council of Canadians with Disabilities v. VIA Rail Canada Inc*., [2007] 1 S.C.R. 650, 2007 SCC 15.

*Gill v. British Columbia (Ministry of Health).* 40 C.H.R.R. D/321, 2001 BCHRT 34.

*Hutterian Brethen of Wilson Colony v. Alberta.* 2007 ABCA 160, affirming *Hutterian Brethen of Wilson Colony* (2006), 33 M.V.R. (5th) 16, 57 Alta.L.R. (4th) 300, 398 A.R. 5 (Alta. Q.B.).

*Kamel v. Canada (Attorney General)*. 2008 FC 338, 2008 CF 338.

*Kerzner v. Minister of National Revenue*. 2005 FC 1574, 10 T.T.R. (2d) 589.

*N.B. v. Canada (Attorney General).* 27 A.R. 135, 40 C.P.C. (4th) 244.

*Naqvi v. Canada (Employment and Immigration Comm.)* [2005] F.C.J. No. 1704, 2005 FC 1392.

*R. v. E. (S.H.)*. 2007 ONCJ 308.

*Sager v. Canada (Minister of Citizenship and Immigration)*. [2005] F.C.J. No. 1704, 2005 FC 1392.

*Turner v. Telus Communication Inc.* 2005 FC 1601, 2006 C.L.L.C. 210-022.

*United States v. Henry*. [2002] O.J. No. 5738, 66 W.C.B. (2d) 104.

*Veffer v. Canada (Minister of Foreign Affairs)*. 2007 FCA 247.

**Other Sources**

"Are Your IDs Secure Enough?" *Digimarc: White Paper*. 2007.

"A Canada–U.S. Border Vision." Canadian Chamber of Commerce. December 2008. http://www.chamber.ca/cmslib/general/blueprint.pdf.

"Armed Forces deploying Biocert Clipbio Pro." *PC Business Products*. Dec 2006, 5–7.

"Canada to Begin Issuing High-Tech Passports." *CTV*, July 18, 2004. http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20040718/canada_passport_040718?s_name=&no_ads=.

"CPA exam now requires fingerprints." *Practical Accountant*, 41 (6) June 2008, 7.

"Ensuring security by managing identity." *Card Technology Today*, June 2005, 12–13.

"Fast-Track Cards a License to Smuggle, Border Guards Fear." *Globe and Mail*, Nov 1, 2008. http://www.theglobeandmail.com/servlet/story/RTGAM.20081101.wbordercar01/BNStory/energy/.

"Further Strengthening of the Use and Verification of Residence Identity Cards." *Chinese Law and Government*, 34 (3) May/June 2001, 90–93.

"Hand Geometry." Subcommittee on Biometrics, National Science and Technology Council. August 7, 2006.

"History of Passports." Passport Canada. http://www.ppt.gc.ca/pptc/hist.aspx?lang=eng.

"Key Accomplishments Since August 2007." Statement from Security and Prosperity Partnership Meeting. New Orleans, U.S., April 22, 2008.

"No fingerprints from under-12s." *Biometric Technology Today*, 16 (10) Oct. 2008, 2–3.

"Passport Canada says Sikh photos rejected by mistake." *CBC News*, Aug 17, 2007. http://www.cbc.ca/canada/british-columbia/story/2007/08/17/bc-passportcanada.html.

"Permanent Resident Card." Citizenship and Immigration Canada. http://www.cic.gc.ca/EnGLIsh/information/pr-card/index.asp.

"Real Time Identification Project" RCMP. http://www.rcmp-grc.gc.ca/rtid-itr/index-eng.htm.

"Security Screening." Canada Border Services Agency. http://cbsa-asfc.gc.ca/security-securite/screen-verific-eng.html.

"Sikh passport photos rejected because of headgear." *CBC News*, Aug. 17, 2007. http://www.cbc.ca/canada/british-columbia/story/2007/08/17/bc-sikhpassports.html.

Acharya, Lalita. "Biometrics and Government." Government of Canada: Parliamentary Information and Research Service. Sept 2006.

Aleksic, Petar S. and Aggelos K. Katsaggelos. "Audio-Visual Biometrics." *Proceedings of the IEEE*, 94 (11), Nov. 2006.

Allan, Roger. “Biometrics looks to solve identity crisis.” *Electronic Design*, 56 (12) June 19, 2008, 31–35.

Ananthaswamy, Anil. “Cracks case doubt on the ‘fussy vault’.” *New Scientist,* Sept. 22, 2007.

Baldassi, Cindy L., DNA, Discrimination and the Definition of Family Class: M.A.O. v. Canada (Minister of Citizenship and Immigration). *Journal of Law and Social Policy*, 21, 2007, 5.

Bhandar, Davina. “Renormalizing Citizenship and Life in Fortress North America.” Citizenship Studies, 8 (3) Sept. 2004, 261–278.

Browne, Simone. “Getting Carded: Border control and the politics of Canada’s Permanent Resident card.” *Citizenship Studies*, 9 (4) Sept. 2005, 423–438.

Burge, Mark, and William Burger. “Ear Biometrics.” In Anil K. Jain et al. eds., *Biometrics: Personal Identification in a Networked Society*. New York: Springer, 2006.

Burns, David R. “Virtual Borders and Surveillance in the Digital Age.” International Journal of Media and Cultural Politics, 3 (3) 2007, 325–341.

Camp, L. J. “Identity, Authentication, and Identifiers in Digital Government.” *International Symposium on Technology and Society*, Sept. 26–28 2003, 10–13.

Canada Border Services Agency. “Documents to Travel to the United States: Chronology.” Nov. 6, 2008. http://www.cbsa-asfc.gc.ca/whti-ivho/chron-eng.html.

Canada Border Services Agency. “Safety and Security: Managing access to Canada.” July 31, 2008. http://www.cbsa-asfc.gc.ca/security-securite/safety-surete-eng.html#s2_1.

Citizenship and Immigration Canada. “Frequently Asked Questions: Biometrics Field Trial.” June 12, 2008. http:/www.cic.gc.ca/english/inFORMation/faq/biometrics/index.asp.

Citizenship and Immigration Canada. “Applying for Citizenship.” http://www.cic.gc.ca/english/citizenship/index.asp.

Connolly, Christine. “Image Processing Algorithms Underpinning Iris and Facial Recognition Systems.” *Sensor Review*, 26 (1) 2006, 22–27.

Covavisaruch, Nongluk, et al. “Personal Verification and Identification Using Hand Geometry.” *ECTI Transactions on Computer and Information Technology*, 1 (2) Nov. 2006.

Daugman, John. “New Methods in Iris Recognition.” *IEEE Transactions on Systems, Man, and Cybernetics*, 37 (5) Oct. 2007, 1167–1175.

Department of Foreign Affairs ans International Trade. “Action Plan for Creating a Secure and Smart Border.” http://www.international.gc.ca/anti-terrorism/actionplan-en.asp.

Deravi, F., et al. “Intelligent Agents for the Management of Complexity in Multi-modal Biometrics.” *Digital Object Identifier*, 2, 2003, 293–304.

Dimauro, G, et al. “Recent Advancements in Automatic Signature Verification.” *Proceedings of the 9th International Workshop on Frontiers in Handwriting Recognition*, 2004.

Dinerstein, Marti. “America’s Identity Crisis: Document fraud is pervasive and pernicious.” *Centre for Immigration Studies,* April 2002. http://www.cis.org/articles/2002/back302.html.

Downes, Stephen. “Authentication and Identification.” *International Journal of Instructional Technology and Distance Learning.* Oct 2005.

Drury, Ian. “ID cards could be derailed by pensioners as finger prints of over-75s are hard to scan.” *The Daily Mail*, Aug. 15, 2008. http://www.dailymail.co.uk/news/article-1045659/ID-cards-derailed-pensioners-finger prints-75s-hard-scan.html.

Egelman, Serge, and Lorrie Faith Cranor. “The Real ID Act: Fixing identity documents with duct tape.” I/S: A Journal of Law and Policy, 2 (1) 2006, 149–183.

Ellison, Carl M. “Establishing Identity Without Certification Authorities.” Presented at *6th USENIX Security Symposium*. San Jose, July 22–25, 1996.

Fairhurst, M. C., and E. Kaplani. “Perceptual Analysis of Handwritten Signatures for Biometric Authenfication.” IEE Proc.-Vis. Image Signal Process, 150 (6) Dec. 2003, 389–394.

Fairhurst, M. C., and S. Ng. “Management of Access Through Biometric Control: A case study based on automatic signature verification.” *Digital Object Identifier*, 1, 2001, 31–39.

Ford, Christopher A. “The Determination of “Race” in Race-Conscious Law.” *California Law Review*, 82 (5) Oct. 1994, 1231–1285.

Gale, Doug. “What’s in a Name?” *T.H.E. Journal*, 33 (11), June 2006, 22–24.

Grijpink, J. H. A. M. “Trend report on biometrics: Some new insights, experiences, and developments.” *Computer Law & Security Report*, 24 (3) May 2008, 261–264.

Gupta, Babita. “Biometrics: Enhancing Security in Organizations.” IBM Center for the Business of Government. 2008.

Hanmandlu, Madasa, et al. “Off-line Signature Verification and Forgery Detection Using Fuzzy Modeling.” *Pattern Recognition*, 38 (3) Mar. 2005, 341–356.

Hashiyada, Masaki. “Development of Biometric DNA Ink for Authentication Security.” *Tohoku Journal of Experimental Medicine*, 204, 2004, 109–117.

Hewitt, Steve. “The Secret History of the Canadian Passport: It’s the preferred choice of discriminating villains everywhere. The question is: why?” *The Beaver*, Apr. 1, 2004.

Ho, Julian. “SCC to Address Accomodation of Religious Freedom Once Again.” *The Court.* Sept 16, 2008. http://www.thecourt.ca/2008/09/16/scc-to-address-accommodation-of-religious-freedom-once-again/.

Holder, Daniel. “More Than Just a Card: Intrusion, exclusion and suspect communities: Implications in Northern Ireland of the British National Identity Scheme.” Northern Ireland Human Rights Commission. Briefing paper prepared for *Identity Cards and Suspect Communities* seminar. Oct 15, 2008. http://www.nihrc.org/dms/data/NIHRC/attachments/dd/files/104/More_than_just_a_card_FINAL.pdf.

Impedovo, S., and G. Pirlo. “Verification of Handwritten Signatures: An Overview.” *14th International Conference on Image Analysis and Processing*, 2007.

International Civil Aviation Organization. “Facilitation and quality of service at airports.” Working Paper, Sept 20, 2004. http://www.icao.int/icao/en/assembl/a35/wp/wp180_en.pdf.

Jacobson, Louis. “Playing the Identity Card.” *National Journal*, Mar. 20, 1999.

Jain, Anil K., Arun Ross, and Sharath Pankanti. “Biometrics: A tool for information seeking.” *IEEE Transactions on Information Forensics and Security*, 1 (2) June 2006.

Jain, Anil K., and Nicolae Duta. “Deformable Matching of Hand Shapes for Verification.” Department of Computer Science and Engineering, Michigan State University, 2007.

Jain, Anil K., et al. eds. *Biometrics: Personal Identification in a Networked Society.* New York: Springer, 2006.

Jain, Anil K., et al. *Handbook of Fingerprint Recognition.* New York: Springer, 2003.

Jain, Anil K., et al. “An Introduction to Biometric Recognition.” *IEEE Transaction on Circuits and Systems for Video Technology*, 14 (1) Jan. 2004.

Jain, Anil, Lin Hong, and Sharath Pankanti. “Biometric Identification.” *Communications of the ACM*, 43(2) Feb. 2000, 90–98

James, Tabitha, et al. “Determining the Intention to Use Biometric Devices: An application and extension of the technology acceptance model.” *Journal of Organizational and End User Computing*, 18 (3) Jul–Sept 2006, 1–24.

Kanellos, Michael. “E-Passports to put new face on old documents.” *CNET*, August 18, 2004.

Karpinski, Maciej Mark, and Charles Théroux. “The Dilemmas of Ensuring National Security while Protecting Human Rights: A Perspective from the Canadian Human Rights Commission.” Canada Human Rights Commission, 2008.

Kittler, J., et al. “Combining Evidence in Personal Identity Verification Systems.” *Pattern Recognition Letters, 18*, 1997, 845–852.

Kochems, Alane, and Laura Keith. “Successfully Securing Identity Documents: A Primer on Preventive Technologies and ID Theft.” *Heritage Foundation: Backgrounder*, No. 1946, June 27, 2006.

Kruger, Erin and Marlene Mulder, Bojan Korenic. “Canada After 11 September: Security measures and ‘preferred’ immigrants.” *Mediterranean Quarterly*, 15 (4) Fall 2004, 72–87.

Landahl, Mark. “Identity Crisis: Defining the problem and framing a solution for terrorism incident response.” *Homeland Security Affairs*, 3 (3) Sept. 2007.

Levine, Jenny. “Biometrics and security.” *Library Journal*, Oct. 15, 2004.

Lodge, Juliet. “Trends in Biometrics.” Briefing Note prepared for The European Parliament’s committee on Civil Liberties, Justice, and Home Affairs. Sept. 28, 2006.

Lyon, David. “Biometrics, Identification, and Surveillance.” *Bioethics*, 22 (9), 2008. 449–508.

Lyon, David. *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination.* London: Routledge, 2003.

McCarthy, Shawn. “No Smiling! We’re Canadian.” *Globe and Mail*, Aug. 27, 2003. http://www.theglobalandmail.com/servlet/story/RTGAM.20030826.wsmile0826/BNStory/National/.

Mcleod, Judi. “Canada Took UN Inspiration for New E-Passport.” *Canadafreepress.com.* July 21, 2004. http://www.canadafreepress.com/2004/main072104.htm.

Michael, K., and M. G. Michael. “The Proliferation of Identification Techniques for Citizen throughout the Ages.” *Faculty of Informatics-Papers*, 2006.

Monk, Bruce. “Designing Identity Documents for Automated Screening.” *2004 IEEE Conference on Technologies for Homeland Security*. Cambridge, MA, April 21–22, 2004.

Muller, Benjamin J. “(Dis)Qualified Bodies: Securitization, citizenship and ‘Identity Management’.” *Citizenship Studies*, 8 (3) Sept. 2004, 279–294.

Negin, Michael, et al. “An Iris Biometric System for Public and Personal use.” *Computer*, 33 (2) Feb 2000, 70–75.

O’Gorman, Lawrence. “Comparing Passwords, Tokens, and Biometrics for User Authentication.” *Proceedings of the IEEE*, 91 (12) Dec. 2003.

Onley, Dawn S. “Biometrics on the front line.” *Government Computer News*, Apr. 16, 2008. http://gcn.com/articles/2004/08/13/biometrics-on-the-front-line.aspx.

Otjacques, Benoit, et al. “Identity Management and Data Sharing in the European Union.” Proceedings of the 39th Hawaii International Conference on System Sciences, 2006.

Pankanti, Sharath, Salil Prabhakar, and Anil K. Jain, “On the Individuality of Fingerprints,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 24 (8) August 2002, 1010–1025.

Passport Canada. “Backgrounder: Refusal or Revocation of Passports.” http://www.ppt.gc.ca/articles/20080213a.aspx?lang=eng.

Pentland, Alex, and Tanseem Choudhury. “Face Recognition for Smart Environments.” *Computer*, 33 (2) Feb. 2000, 50–55.

Privy Council Office. “Securing an Open Society: Canada’s National Security Policy.” April 2004.

Roethenbaugh, Gary. “Biometrics Explained.” *International Committee for Information Technology Standards*. Sept. 2005.

Rosenzweig, Paul, Alane Kechems, and Ari Schwartz. “Biometric Technologies: Security, legal, and policy implications.” *Legal Memorandum: The Heritage Foundation, 12*, June 21, 2004.

Ross, Arun, and Anil Jain. “Information Fusion in Biometrics.” *Pattern Recognition Letters*, 24 (13) Sept. 2003, 2115–2125.

Roy, Bjorn. “A Case Against Biometric National Identification Systems (NIDS): “Trading-Off” privacy without getting security.” *Windsor Review of Legal and Social Issues, 19* (45) March 2005.

Sanchez-Reillo, Rand, and Ana Gonzalex-Marcos. “Access Control System with Hand Geometry Verification and Smart Cards.” *IEEE AES Systems Magazine,* Feb. 2000.

Security and Prosperity Partnership. “Fact Sheet: Security and Prosperity Partnership of North America.” March 31, 2006.

Sinoski, Kelly. “Passport Canada apologizes for refusing passports to Sikhs.” *Vancouver Sun,* Aug. 18, 2007 on Nov. 18, 2008.

Soutar, Colin. “Implementation of Biometric Systems: Security and Privacy Considerations.” *Information Security Technical Report, 7* (4) 2002, 49–55.

Sparke, Matthew B. “A Neoliberal Nexus: Economy, security and the biopolitics of citizenship on the border.” *Political Geography, 25*, 2006, 151–180.

The White House. “Specifics of Secure and Smart Border Action Plan.” Jan. 7, 2002. http://www.dhs.gov/xnews/releases/press_release_0036.shtm.

Thomas, Rebekah. “Biometrics, International Migrants, and Human Rights.” *European Journal of Migration and Law, 7,* 2005. 377–411.

Toledano, Doroteo T., et al. “Usability Evaluation of Multi-modal Biometric Verification Systems.” *Interacting with Computers, 18* (5) Sept. 2006, 1101–1122.

Torpey, John. “The Great War and the Birth of the Modern Passport System,” in Jane Caplan and John Torpey, eds., *Documenting Individual Identities: The Developments of State Practices in the Modern World.* Princeton: Princeton University Press, 2001, 256–270.

Tuller, Mike, et al. “Biometrics: Strategic Technology Analysis.” Technology Foresight Dynamics, Group 4 White Paper, 2006.

UK Passport Service. “UKPS Biometrics enrollment trial report.” May 2005. http://hornbeam.cs.ucl.ac.uk/hcs/teaching/GA10/lec3extra/UKPSBiometrics_Enrolment_Trial_Report.pdf

Wang, Jia-Ching, et al. “Robust Speaker Identification and Verification.” *Computational Intelligence Magazine, IEEE, 2* (2) May 2007, 52–59.

Wayman, James L. “Fundamentals of Biometric Authentication Techniques.” *International Journal of Image and Graphics, 1* (1) 2001, 93–113.

Whitaker, Reg. “Securing the ‘Ontario–Vermont border’: Myths and Realities in Post-9/11 Canadian–American Security Relations,” *International Journal*, *60* (1) Winter 2004–2005, 53–70.

Wigan, Marcus. “Owning identity—one or many—do we have a choice?” in The Second Workshop on the Social Implications of National Security. Australian Homeland Security Research Centre, October 2007.

Williams, Brent C., et al. “The Accuracy of the National Death Index When Personal Identifiers Other than Social Security Number are Used.” *American Journal of Public Health*, *82* (8) Aug. 1992, 1145–1147.

Wilson, Dean. “Biometrics, Borders, and the Ideal Suspect,” in S. Pickering and L. Weber, eds., *Borders, Mobility, and Technologies of Control*. Netherlands: Springer, 2006, 87–109.

Yoruk, Erdem, Helin Dutagaci, and Bulent Sankur. “Hand Biometrics.” *Image and Vision Computing*, *24* (5) May 2006, 483–497.