

Biometric Authentication and Identification Systems for Border Controls: A look at U.S. and Canadian Programs

Numerous media reports over the past couple of years have highlighted recent U.S. and Canadian efforts to strengthen border security.¹ These efforts have involved the implementation of numerous new initiatives under an overarching bi-lateral agreement known as the Smart Border declaration.² Central to the Smart Border agreement is the use of biometric identifiers. Most U.S. initiatives are part of a program known as USVISIT (United States Visitor and Immigrant Status Indicator Technology) while Canada has a number of smaller programs. When fully implemented the USVISIT program will see the most expansive use of biometrics as a security tool in the world, utilizing integrated hardware, databases, enforcement measures, and other tools.³ Fundamental to both Canadian and U.S. programs is the use of biometric identifiers in new machine-readable “smart” travel documents such as visas, permanent resident cards, and passports. The implementation timetable for these programs was considerably accelerated in the days following the September 11, 2001 terrorist attacks.

Current biometric technology, while useful in many aspects of border security offers only very specific and limited assistance to anti-terrorist activities. Thus the vast investment of fiscal resources may be a mistake if a belief that such systems will provide a surefire barrier to terrorists trying to enter the country exists. Notwithstanding the rhetoric of homeland security surrounding the Smart Border declaration and the USVISIT program, the use of biometrics brings to light a number of possibilities and controversies. As a method of introduction this paper will primarily examine the USVIST program and briefly touch on emerging Canadian use of biometrics in order that the nascent programs can be properly assessed for their anti-terrorist potential. This paper will only examine the technological aspects of the programs. Much else remains to be studied, including the civil liberty implications, detailed cost-benefit analysis, and potential trade disruption.

Biometrics is defined as “a measure of an individual’s unique physical or behavioral characteristics to recognize or authenticate identity.”⁴ The use of biometrics in wide-scale border security programs is controversial for several reasons, not the least of which is the overall effectiveness of such programs when a main goal is stopping terrorists unconcerned about their own survival. Initial development and implementation costs (exclusive of recurring expenses) of USVISIT were originally estimated in the USD\$3.8 billion range.⁵ The most recent estimates now peg the figure at a maximum of USD\$15 billion.⁶ In Canada, rough estimates place the amount in the range of CDN \$2 billion.⁷ These estimates include some, but not all, of the recurring costs involved. Given the vast monetary resources being committed it is necessary to ponder the effectiveness such a program would have in countering the types of threats facing North America today.

Biometrics for the purposes of identification and authentication is not a concept born solely of the September 11 catastrophe. For example, the NEXUS program to facilitate accelerated movement of approved frequent travelers began in 1999.⁸ The U.S. in particular sought an early lead in the use of such technologies through, “a series of laws enacted between 1996 and spring 2002 [that required] the Federal government to develop Chimera, an automated information system, to gather and share information among agencies about aliens seeking to enter and stay in” the country.⁹ The Chimera

system consists of three major components: biometric identifiers, machine-readable documents with embedded biometrics, and interoperability among a broad range of U.S. and now Canadian security and law enforcement departments.¹⁰ In Canada and the U.S. recent legislation has clearly defined both mandate and the types of biometric technology to be used for border security. The primary legislative acts include the USA Patriot Act, the Enhanced Border Security and Visa Entry Reform Act of 2002 (Border Security Act),¹¹ and the Canadian Anti-Terrorism Act.¹²

Various biometric systems have been in use by different agencies across the world for several years now. The largest system coupled to a database is the FBI's Automatic Fingerprint Identification System (AFIS) which has been operating for over 30 years.¹³ While automated, AFIS is not similar to systems proposed for border control in that matches are generally confirmed by manual human inspection. Systems for border control would ideally operate with minimal human inspection. That being said, a number of small automated systems are in operation. Among others, the U.S. Defense Department has used biometric fingerprint identification for access to military bases in South Korea¹⁴ and, since 2002, the U.S. Immigration and Naturalization Service (INS) has been using a hand geometry system on a very limited basis to reduce inspection times for trusted travelers at seven U.S. and two Canadian airports.¹⁵ As well, Canada is running programs such as CANPASS (Canadian Passenger Accelerated Service System) at a number of airports and other points-of entry (POE). Many European Union members also have biometric authentication and identification systems operational at various POE.

It is important at this point to clarify the differences in identification (also called recognition) and authentication (or verification). Dr. George Tomko, a leading Canadian researcher in the field of biometric photonics, describes the identification process as "matching a physiological or behavioral characteristic of a person to an established and pre-confirmed record."¹⁶ This process is also known as a "one-to-many" (or "1:N" in scientific terms) search. For border security applications, this would mean that an applicant for a visa, passport, or permanent resident card, would have to submit to a fingerprint, iris, or facial scan that can be used as a positive identifier for the purposes of the application.

Once in a system database, the submitted identification characteristics would be used to authenticate that individual after documents have been issued. Dr. Tomko likens the authentication process to the use of a Personal Identification Number (PIN) for bank machine access.¹⁷ Whenever a person who has been issued travel documents wishes to cross a border point-of-entry, they would undergo an authentication process involving a scan and matching of biometric characteristics that exist in a database. This is also known as a "one-to-one" or (1:1) search.¹⁸

It must be clearly understood that the whole premise of biometric security is founded upon the existence of an extensive and accessible database. Thus, while biometric data stored in a machine-readable travel document will decrease the likelihood of document fraud, the machine readability of the document is worthless without a related database. This type of system is known as positive identification; anyone with a biometric travel document would be present in a database.¹⁹ This type of system is common in high-security access systems in private industry and would allow fast and accurate screening of people crossing the border. The time it takes to screen travelers is crucial; undue delays would constitute an intolerable hindrance to trade. One of the major

justifications for machine readable documents is that they can be quickly screened at the POE without requesting a physical submission of biometric data from each individual. The only situation in which this would occur would be if the system alerts border personnel to a non-match reading of the documents.

A second option for the use of machine-readable documents is negative identification. A negative identification system is “designed to ensure that a person’s biometric information is not present in a database” or a watch list.²⁰ Negative identification systems, especially when generally termed by media with the catch-all phrase of watch lists, are often portrayed in a negative light because of questions of racial profiling and the secrecy of the administrative process behind such lists. The point is that regardless of the system employed, without a database any biometric system is handicapped and essentially useless as a method of border security.

This begs a serious and largely unanswerable question. When a person is applying for a travel visa, passport, asylum, or refugee status, how do authorities verify that the identification being presented, if any, is authentic? This problem is especially acute when dealing with people originating from countries that do not have reliable documentation systems or when processing refugees from catastrophic natural disasters or chaotic war zones.

The rapid expansion internationally of large-scale public biometric programs created a need for standardization of technological specifications. The ISO (International Organization for Standardization) and ICAO (International Civil Aviation Organization) have published standards to be met by members that allow commonality between systems.²¹ The National Institute of Standards and Technology (NIST) branch of the U.S. Dept. of Justice took an early and lead role in the development of those standards, identifying three key biometric systems considered to be most applicable (in light of current technology) to border security as being “fingerprint matching for identification, single-finger flat fingerprint verification, and face-based verification.”²² The NIST recommends a system of identification based on “at least two fingerprints to positively identify visa applicants” and a system of authentication based upon “a dual system of face and fingerprints to verify the identities of visa holders.”²³ Given the accuracy of current technology a number of scientists have pointed out that “biometric systems based solely on a single biometric may not always meet performance requirements.”²⁴ The easiest solution to this is the use of multi-biometrics—in essence, “data from multiple and independent biometric identifiers are fused; reinforcing the identity of a subject.”²⁵

The Border Security Act, passed in 2002, mandated that the U.S. State Department, Justice Department, and Department of Homeland Security have machine-readable visas, passports, and related systems in the field and operating by October 2003.²⁶ This timetable was very ambitious and was largely a result of the 9/11 attacks. The USVISIT program was created to fulfill this mandate and, although slightly behind schedule, was declared operational on 5 January 2004. Complete deployment is due by the end of 2005.²⁷ The USVISIT program currently requires fingerprint scans and digital photographs and thus lacks multi-biometric safeguards. Only the data from the electronic fingerprints are stored in the CHIMERA database. Facial recognition technology was chosen as the second biometric because it “is the only biometric that can be used for surveillance purposes”²⁸ which would ultimately allow active automated surveillance of border crossings. However, numerous scientific, industry, and independent sources point

out the inaccuracies of current facial recognition technology, especially in conditions of outdoor lighting.²⁹ Similar challenges exist for database scanning of stored digital images which relegates the use of facial technology to some unknown future date.

USVISIT is the most ambitious biometric program ever deployed, involving the collection of digital information as part of the visa application process at all U.S. embassies, consulates, and POE. However, there are several categories of exemptions, the largest of which include Canadian and Mexican nationals. This is problematic for several reasons, primarily because the vast majority of visitors to the U.S. originate from its two closest neighbors, comprising “about 78 percent of the entries from land, sea, and air.”³⁰ Although recently passed legislation will force all entrants to the U.S. (including its own citizens) to present valid passport identification, the new measure is only in the public consultation phase of implementation.³¹ This constitutes a huge gap in the USVISIT scheme.

As noted earlier, biometric technology has been used for several years commercially and by a number of governments on a limited scale. None of the aforementioned applications approach the vast scale intended for Chimera/USVISIT. The short development and implementation schedule allowed by the Border Security Act and the Homeland Security Act forced the U.S. government to have “specific interest in off the shelf technologies that have immediate application” in order to “protect the greatest part of the border in the least amount of time.”³² This dependence on existing technologies, which have been proven to be less accurate than what is considered necessary, has fueled criticism of the programs.

In her testimony to a Senate subcommittee, Nancy Kingsbury, Managing Director of the U.S. General Accounting Office’s Applied Research and Methods Branch, stated that “questions remain regarding the technical and operational effectiveness of biometric technologies in applications as large as border control.”³³ The rush to have an operable system in place by the end of 2003 brought two major operational concerns to the fore. First, the effectiveness of having only a single-system (fingerprint) based program and second, the system limitations with respect to false match (FMR), false non-match (FMNR), and failure-to-enroll (FTE) rates of the technologies currently available.

To reduce error probability, USVISIT was to rely upon a multi-faceted system of identification and authentication. Having to rely solely on the dual (two finger) fingerprinting system for automated use and digital photographs that require manual confirmation handicaps the program. This problem exists largely because of the accelerated deployment timetables and the ultimate goal of having automated real-time surveillance capability. While the ultimate goals of the program are impressive, the potential short to mid-term problems that could arise because of this may ultimately harm the integrity of the system.

The projected rate of error is the second major issue that facing USVISIT. As Kingsbury has reported, “if the biometric technology that is used...has a high rate of false matches...processing workload could increase... [and]...it could lead to increased delays in the inspection process.” She continues: “Exception processing will also have to be carefully considered...processing that is not as good as biometric based primary processing could be exploited as a security hole.”³⁴ Dr. Kingsbury’s concerns have been echoed by other experts. Dr. Tomko has spoken of error rates as high as 30% being possible with the current fingerprint-scan technology.³⁵ Others have cited error rates as

low as 1%³⁶ but the USGAO's own competition test results for various fingerprint analysis algorithm error rates range from as low as 0.19% to highs of 50%.³⁷ The most recent NIST sponsored Fingerprint Verification Competition, FVC2004, produced average operational error rates at roughly 2%, a rate, one set of authors point out, that would result in 4000 false rejects per day if deployed in the New York City Airports as a sole-technology biometric system.³⁸

The rate of border inspections is anticipated to be in the range of 500 million annually.³⁹ Therefore, the potential number of false-match and false non-match scans is enormous. This could leave "millions of people vulnerable to mistaken identity" and "long line-ups at airports...because [people] have been wrongly flagged by a biometric scanner."⁴⁰ Although this worse-case scenario has yet to occur, the potential remains and demands consideration when pondering major problems that could arise. Concomitant to this is the NIST report that "it is not possible to obtain a good quality fingerprint from approximately two percent of the population and hence such people cannot be enrolled in a fingerprint biometric system."⁴¹ This situation most often occurs when dealing with people who work at manual labour jobs, such as trades-people or farmers, or those who have suffered from accidental damage to fingers and hands from burns, chemicals, and other agents. Given that many refugees and those forced by regulation to submit to enrollment in USVISIT would fall into one of the above categories, the FTE rate could prove a major obstacle to single-biometric system.

A final problem with the use of fingerprints as a sole biometric is the fact that it has never been scientifically established that fingerprints are indeed unique. A group of influential scientific experts point out that "the notion of fingerprint individuality has been widely accepted based on manual inspection (by experts) of millions of fingerprints. Despite this, the fact remains that the "scientific basis of fingerprint individuality has not been rigorously studied or tested."⁴² Dr. Kingsbury echoes this concern. In her landmark 2002 report she states that "it has never been formally established by scientific means that a person's fingerprints are unique. Because it is impossible to obtain the fingerprints of every person in the world, estimating fingerprint individuality requires statistical methods to project the probability (emphasis added) that two people will have the same fingerprint."⁴³ This fact may seem trivial to many but the point remains that there has been little formal study of the assumptions of individuality of fingerprints. USVISIT pushes the limits of technology; it would be imprudent to ignore questions that challenge a fundamental assumption upon which the program is founded. With such daunting technological and operational hurdles, the effectiveness of the program in actually combating the current terrorist threat remains in question.

In September 2003, the C.D. Howe institute held a closed seminar consisting of a broad panel of government, business, and academic experts from the U.S. and Canada. The purpose of the seminar was to examine the long-term implications of various terrorist threats on Canada and the United States. Some of the threats discussed include biological and radiological attacks, an attack on energy infrastructure with an aircraft, and the threat of a car-bombing type of assault against a busy U.S. airport.⁴⁴ Potentially, all of these threats would involve the deaths of the perpetrators during the assaults, which would be consistent with the type of terrorist activity that has recently taken place in areas as divergent as Moscow, Israel, Iraq, Sri Lanka and New York.⁴⁵ The question to be considered here is how USVISIT, or any comparable Canadian program stop or prevent

such an attack? Consider the fact that all of the September 11th hijackers had legally obtained U.S. visas.⁴⁶ The USVISIT system database “does not change the paradigm by which visas are granted—the process will still only look to the existence of negative information that indicates links to international terrorism; any individual not specifically identified as a terrorist in government databases will be granted entry.”⁴⁷

While the system is intended to be accessible or “mined” by all law enforcement and security agencies in the U.S., it does not “allow the government to know where an alien is or intends to be; as such, subsequently garnered information of terrorist links or evidence of noncompliance with visa terms cannot be acted on.”⁴⁸ To the credit of the U.S. government several programs concomitant with USVISIT are now more or less operational to deal with this obvious gap in the immigration system.⁴⁹ The lack of interoperability between various agency databases was a contributing factor to the attacks on New York and Washington, and this deficiency would theoretically be overcome by the CHIMERA database. However, the system alone would lack the ability to confirm an alien’s compliance with the terms under which a legal visa had been issued. This underlines the fact that a biometric program can only be a single component in a greater security system. Proper use of the information provided by the overall security net would remain essential for enforcement of visa compliance.

The inability to confirm compliance with visa conditions and the absence of a method of verifying the whereabouts of the September 11th hijackers was a contributive factor to that day’s events.⁵⁰ Considering this type of threat, a potential suicide attacker only needs to legally enter the system once. Furthermore, the integrity of the system is based upon legitimate identification being introduced into the system at the enrollment stage of the visa issuance process, a problematic issue already discussed. A person could quite easily present false credentials at the enrollment stage. As Keith Rhodes has pointed out, “biometrics would make it difficult for people to establish multiple identities” but once in a system a person could be linked to a false identity, facilitating criminal activity.⁵¹

It is highly unlikely that a terrorist or criminal would use their true identity on a visa if an alias would further the chances of success; indeed, documents attributable to al Qaeda point to the value of aliases in terrorist activity.⁵² Furthermore, a number of the perpetrators of the London bombings of 2005 were either born in the UK or Commonwealth countries or naturalized citizens; as such none were known as terrorists or extremists until after the fact.⁵³ To USVISIT, such people may not have any identifiable terrorist links or indeed even be in the system. With such massive outlay of finite monetary resources one must wonder what benefits, if any, biometric systems would have in countering a terrorist threat.

As part of a multi-layered approach to domestic security, biometric systems can play an indispensable role. However, the role may be an indirect rather than primary one as touted by government press releases and other advocates. Sophisticated terrorist activity will use any and all loopholes to great advantage. One useful purpose of USVISIT could be the detection of known “organizers of international terrorism: recruiters, couriers, fundraisers,”⁵⁴ the permanent staff of major terrorist groups. Janice Kephart’s study of terrorist activity in the U.S. from the 1990s to 2004 clearly elucidates the important role these organizers play in global terrorist networks.⁵⁵ Presumably, if

operating in the U.S., this permanent staff would have to enter the system more than once since their role is not that of a suicide attacker.

Biometric systems would also cut down on the production of fraudulent documents and thus hinder the use of multiple passports and visas. Once identified and tied to a particular identity, the system should catch those trying to slip through using an alias or documents that are not attributed to a particular individual. Thus, would-be terrorists such as Nageeb Abdul Jabar Mohamed Al-Hadi, who was arrested carrying multiple Yemenese passports with differing names and birthdates on September 11th 2001, would be caught not by chance, as it occurred, but as a matter of course.⁵⁶ While not ensuring that the initial identity presented is valid, the use of embedded biometrics will serve to exponentially increase the security of documents themselves, currently a major problem in both the U.S. and Canada.⁵⁷

Terrorists could still slip across the Canada-U.S. border without being flagged by any biometric system. For example, it is unlikely that, were it not for his own ineptness and an alert U.S. border guard, Ahmed Ressay, an Algerian born French national residing in Canada on a refugee claim, would have been identified by USVISIT because he was traveling with a valid Canadian passport.⁵⁸ Ressay was intent on bombing Los Angeles International airport and was linked to the GIA, and Algerian Islamic terrorist group. Ressay had fraudulently obtained his passport using an alias, a situation that may or may not be possible with embedded biometrics, depending on circumstances. Regardless, traveling with valid Canadian documents Ressay would have been exempt from automatic inspection at the U.S. border. No amount of biometric identification would have helped detain Ressay while large exemption categories exist in USVISIT unless mandatory screening of every traveler was enforced.

Beyond the terrorist threat, there are useful purposes for USVISIT and biometrics. Criminals who are wanted on various charges either domestically or internationally would be readily identified if the database is mined as intended by law enforcement officials and border control agencies. Before the program was initiated in January 2004, “a two-month test program in Atlanta caught 21 people (out of 20 000) wanted on various charges, including rape and immigration fraud.”⁵⁹ In the first month after the program was officially initiated on 5 January 2004, a further 30 wanted persons were apprehended, including suspected and convicted drug traffickers, murderers, and others travelling on false documents. The people captured originated from, among other places, the U.S., Peru, and China.⁶⁰ The ultimate value of biometric systems may in fact lie in the area of traditional law enforcement rather than anti-terror activities. A key consideration that is often overlooked when such figures are produced though is the fiscal resources expended to nab this extremely small number of people—21 out of 20 000 is .001%! What price security? Even if the number of criminals apprehended in a year eventually lays in the low thousands is the expenditure of billions justified?

On the Canadian side, there seems to be a fair degree of government waffling on the construction of a comprehensive border security system utilizing biometrics that is integrated with law enforcement agencies. Canada has implemented a number of useful programs in cooperation with the U.S., in particular the aforementioned NEXUS and FAST programs. As well, the CANPASS program enrolls frequent travelers using highly accurate iris biometric technology.⁶¹ Soon, a six month pilot project using biometrics

with integrated databases and watch lists will be launched.⁶² With the exception of this newest program, all require voluntary rather than compelled enrollment.

Canada has committed to updating its passport with embedded biometric data stored on a computer chip. Theoretically this would overcome the long standing problem of fraudulent travel document production. Finally, the long awaited deployment of the LiveScan and related Real Time Identification (RTID) system has begun which will see the collection of digitized fingerprints from refugee claimants and suspect individuals that will be processed electronically rather than manually, as had been done in the past.⁶³ All of the above initiatives are laudable but huge gaps and inconsistencies in the Canadian program remain.

Sheila Fraser, the Auditor General of Canada released a follow-up to the March 2004 report in April of 2005.⁶⁴ Her newest report, while giving approval to the Government's efforts to rectify the deficiencies identified in March 2004, points to some glaring problems with the issuance of passports and transportation security in general. With respect to passports, the report notes that the lack of direct electronic links to various databases hinders the provision of secure documents. This includes automatic links to various watch lists, a seemingly critical component of the issuance process, and provincial databases for the validation of basic personal information such as date of birth or confirmation of death.⁶⁵ Moreover, the report identified deficiencies in the training provided to overseas consular staff in the examination, approval, and printing process for passports. Given that some 100 000 passports are issued annually at consulates and embassies abroad this is inexcusable. Overseas consulates are also hindered by the lack of automatic and direct electronic links to vital information in databases located in Canada.

The Auditor General's conclusions in Chapter three of the report are damning: "The Passport Office is struggling to balance and meet increasing security expectations...The Passport Office cannot effectively authenticate an applicant's identity and determine eligibility...Its watch list is deficient...It has not found ways to automatically obtain necessary data from other government sources, or ways to effectively validate identity data with the provinces..."⁶⁶ In short, the Passport Office is unable to perform the vital functions of its mandate. Not only is this an embarrassing hole in Canada's basic security, it provides fuel to critics abroad who believe that Canada is a haven for terrorist activity.⁶⁷

The Auditor General's report is somewhat more positive in its analysis of the various transport security programs now in place but indicates that much work remains to be done. Particular concern lies with the interoperability of information systems used by various agencies. The March 2004 report found that "the government had failed to improve its security information systems to ensure that they could communicate with each other" and "a lack of coordination of intelligence."⁶⁸ The common problem faced by the agencies responsible for transportation security (including the screening of airline passengers) is the inability to access information and intelligence relevant to the mandate of the agencies. All the biometric systems currently being deployed in Canada are essentially useless, or at the very least extensively handicapped to the point that effectiveness is questionable, by the lack of a central database that can be accessed in a reasonable amount of time. In short, while document security will be improved by the inclusion of biometrics and electronic fingerprinting are benefits in and of themselves,

the lack of a database of at least comprehensive watch lists leaves Canada almost as vulnerable as it ever was.

Criticisms of biometric programs and USVISIT in particular come from a number of directions. First there are staunch advocates of biometrics for border control who argue that deployment is not proceeding fast enough. Second are those who point to privacy concerns, the lack of transparency in the construction of watch lists, and potential database insecurity, among other issues. Those in the first group prefer to either not acknowledge or gloss over problems of technology, instead pointing to the potential benefits or the current lack of actual operational problems. For example, two scholars, Rosemary Jenks and Steven Camarota assert in a 2003 article that “the fact that the administration has failed to meet more than half of the deadlines that have passed so far...indicates a disturbing lack of commitment on the part of the administration to secure our homeland from those who wish us harm and to uphold its Constitutional duty to ensure that the laws of the United States are faithfully executed.”⁶⁹ Rather than pointing out, as Randolph Hite of the USGAO does, that the technological hurdles are immense and that “US-VISIT is a large, complex, and expensive program aimed at supporting a multifaceted mission-critical area [and therefore] it is an intrinsically challenging effort”⁷⁰ with attendant risks, Jenks and Camarota prefer to challenge the commitment and patriotism of the very administration that sponsored the accelerated implementation timetable.

Jessica Vaughan, another critic on the lines of Jenks and Camarota, has used spurious analogies to bolster her criticisms of the U.S. government. For example, she makes an equation between the New Jersey State EZ-Pass system, which uses radio frequency identification technology to toll users of the New Jersey Turnpike, and USVISIT’s proposed exit recording system which has yet to be deployed.⁷¹ There are few similarities between the systems. First of all, the EZ-Pass system is a voluntary program in which users relinquish a small amount of privacy for the convenience of quicker travel. People enrolled in USVISIT are compelled to enter a system that sees their information lodged in a massive database accessible to a wide range of authorities. Furthermore, Vaughan neglects to point out that the EZ-Pass system has at various times been grossly over budget, its database vulnerable to hackers, and has erroneously identified, billed, and fined users.⁷² Comparison to the FAST or NEXUS programs would be apt; comparison to USVISIT is not. While many of Vaughan’s arguments in her numerous papers are sound her choice of example in this instance is unreasonable.

The second group of critics point to privacy and legal implications. Concerns over biometrics and privacy have come from Dr. Kingsbury, Dr. Tomko, Dr. Ann Cavoukian, Jennifer Stoddart, and many others.⁷³ However, initial public concerns over the use of such technologies seem to have been overcome by the increased in personal security and privacy allowed by counterfeit resistant documents that utilize embedded biometrics.⁷⁴

Perhaps the most reasoned argument comes from Paul Rosenweig, Alane Kochems, and Ari Schwartz. In an article entitled “Biometric Technologies: Security, Legal, and Policy Implications,” the authors, while generally supportive of biometric programs, contend that those who vociferously argue for or against biometrics are equally mistaken. Rather, they assert persuasively that “the true policy challenge is in finding the most effective uses of the specific biometric technology—both for liberty and security—not in labeling it as universally good or evil.”⁷⁵ Their argument acknowledges the

benefits and potential pitfalls while being mindful of current technological limitations as well as ongoing scientific research and development.

As currently constructed, the USVISIT program or any of the Canadian programs alone will be unable to deal with the most salient threats faced by the U.S. or Canada. As long as the role and potential of biometrics in a comprehensive, multi-layered border security program is clearly understood then the funds being expended may be justified in the long term. However, the resources being expended are unlikely to have a major anti-terrorist impact, which is counter to current U.S. and some Canadian justifications for the programs. Other security initiatives such as visa policy coordination, cooperation with refugee processing, new maritime security policies, and increased container inspections at seaports are likely to play a more vital role in North American security given current technological limitations.⁷⁶ Undue expectations and reliance on biometric border security programs it is likely to engender a false sense of security. While the benefits of biometrics are clear, the limits of the technology are equally apparent. With the exception of the passport office difficulties noted above, Canada's limited use of biometrics in limited programs constitutes a more reasoned use of biometrics than USVISIT.

This paper has examined only a fraction of the controversies and possibilities surrounding the biometric border security system being implemented by the U.S. and Canada. There are serious issues that need to be addressed rationally and thoughtfully by citizens, government, and academics that are beyond the limited scope of this paper. Perhaps one of the most important issues is the potential economic impacts of such programs. It has been postulated that effects on travel and tourism could be heavy.⁷⁷ In fact, Statistics Canada has already cited border security delays as a real factor hampering cross-border trade.⁷⁸ Other issues touched on but not deeply explored in this paper include privacy rights, misidentification issues, control of database information and database security. Until such a time that these issues and technological challenges are overcome, biometrics, while useful for many applications, will not be an effective anti-terrorist tool.

Endnotes

¹ For example: "Bio-security still a fantasy: Airport screening won't work." The Toronto Star, 24 January 2004. www.thestar.com, Paul Knox, The Globe and Mail. Toronto. 7 February 2004. p.A10., "U.S. passport plan draws fire," The Globe and Mail: Toronto. 6 October 2005, p.A16., and "Prime Minister inaugurates new border facilities in Beauce region,"

<http://www.newswire.ca/en/releases/archive/October2005/14/c1180.html>

² The complete Smart Border Declaration is available at: <http://www.dfait-maeci.gc.ca/anti-terrorism/actionplan-en.asp>. Status updates are available at: <http://www.dfait-maeci.gc.ca/world/site/includes/print.asp?lang=en&print=1&>

³ For a proper grasp of the program see Nancy Kingsbury, Technology Assessment: Using Biometrics for Border Security. United States General Accounting Office (USGAO), report #GAO-03-174, November 2002. <http://www.gao.gov/new.items/d03174.pdf>. For the attendant risks brought about by the scale of the program: Randolph C. Hite, Homeland Security: Risks Facing Key Border and Transportation Security Program Need to Be Addressed. Washington D.C.: U.S. General Accounting Office, Report GAO-04-569T. <http://www.gao.gov/new.items/d04569t.pdf>

⁴ Stern, Shirley Ann, "Oracle and Biometrics," Oracle White Paper, January 2004. Redwood Shores, CA. http://www.oracle.com/technology/depoy/security/pdf/biometrics_twp.pdf Accessed 4 October 2005. There are numerous definitions used by different actors involved in the development and deployment of biometric systems for border control. Fundamentally, all acknowledge that biometrics are unique individual traits that can be used for identification purposes.

⁵ Kingsbury, Nancy, "Border Security: Challenges in Implementing Technology." Testimony before the Subcom. On Terrorism, Technology, and Homeland Security, 12 March 2003. USGAO report #GAO-03-546T. <http://www.gao.gov/new.items/d03546t.pdf> p.11. Accessed 6 February 2004.

⁶ Hite, Randolph C., Homeland Security: Risks Facing Key Border and Transportation Security Program Need to Be Addressed. Washington D.C.: U.S. General Accounting Office, Report GAO-04-569T, p.10. <http://www.gao.gov/new.items/d04569t.pdf> Accessed 3 October 2005.

⁷ It is difficult to differentiate the costs of individual biometric security programs in Canada due to the number of departments involved and the number of programs. However, it is possible to estimate based on the Federal 2001, 2003, 2004, and 2005 budgets and the 2004 and 2005 reports of the Auditor General to Parliament. Budgets are available at: <http://www.fin.gc.ca>, Auditor General Reports are available at: www.oag-bvg.gc.ca.

⁸ <http://www.fhwa.dot.gov/uscanada/issues/nexus.htm>

⁹ Kingsbury, Nancy, Technology Assessment: Using Biometrics for Border Security. United States General Accounting Office (USGAO), report #GAO-03-174, November 2002. <http://www.gao.gov/new.items/d03174.pdf> p.19. Accessed 13 February 2004.

¹⁰ Ibid.

¹¹ Ibid., (footnote 2)

¹² Canadian Department of Justice, Backgrounder, "Highlights of Anti-Terrorism Act." 24 April 2003. http://canada.justice.gc.ca/en/news/nr/2001/doc_27787.html. Accessed 30 January 2004.

¹³ Jain, A.K., et al, "Biometrics: A Grand Challenge," Proceedings of International Conference on Pattern Recognition, Cambridge, U.K., August 2004. <http://biometrics.cse.msu.edu/biometricsgrandchallenge.pdf> p.2. Accessed 4 October 2005.

¹⁴ Walker, Richard, "Security: Biometrics Gains a Foothold" 5 May 2003. <http://www.gcn.com/cgi-bin/udt/im.display> (Post-Newsweek Media Inc.)

¹⁵ Kingsbury, 2003. p.4.

¹⁶ Tomko, 1998.

¹⁷ Ibid.

¹⁸ There are a number of publications that provide greater depth to the authentication and identification process than what can be presented in this paper. They include Kingsbury, 2002, pp.41-45, John Woodward, et al, Biometrics: A Look at Facial Recognition, Rand Corporation: Arlington, 2003, p.2, and Background Material on Biometrics and Enhanced Network Systems for the Security of International Travel, OECD: Paris, 23 December 2004, p.24; full document available at: <http://www.oecd.org/dataoecd/16/18/34661198.pdf> Accessed 3 October 2005.

¹⁹ Rhodes, Keith A., Information Security: Challenges in Using Biometrics. USGAO Report # GAO-03-1137T. USGAO: Washington D.C. 9 September 2003. p.5. <http://www.gao.gov/new.items/d031137t.pdf> Accessed 5 October 2005.

²⁰ Ibid.

²¹ "New International Standards on Biometric Data for ID Systems would Support Controversial UK Initiative," 30 August 2005. http://www.ansi.org/news_publications/news_story.aspx?menuid=7&articleid=1026 Accessed 5 October 2005.

²² Bement, Arden, "S 1749/HR 3525 Enhanced Border Security and Visa Entry Reform Act." Statement to the Subcommittee on Immigration Committee on the Judiciary, United States Senate. 12 April 2002. <http://www.nist.gov/testimony/2002/abvisa.html>. Accessed 24 January 2004.

²³ NIST press release. "NIST Supports Multiple Biometrics for Border Security." 18 February 2003. <http://govtsecurity.securitysolutions.com/microsites/newsarticle>. Accessed 24 January 2004.

²⁴ Rhodes, p.13.

²⁵ Jain, Anil K., et al, "Biometrics: A Grand Challenge," Proceedings of International Conference on Pattern Recognition, Cambridge, UK, August 2004. p.6. <http://biometrics.cse.msu.edu/biometricsgrandchallenge.pdf> Accessed 4 October 2005.

²⁶ Strickland, Lee and Jennifer Willard, "Reengineering the Immigration System: A Case for Data Mining and Information Assurance to Enhance Homeland Security." Homeland Security Journal, October 2002. <http://www.homelandsecurity.org/journal/Articles/Strickland.html> p.16. Accessed 6 February 2004.

²⁷ Press Release: "US VISIT Begins Deployment of Biometric Entry Procedures to Additional Land Border Ports of Entry with Canada and Mexico," 26 September 2005.

<http://www.dhs.gov/dhspublic/display?theme=43&Content=4858&print=true> Accessed 10 October 2005.

²⁸ Rhodes, p.7.

²⁹ Stern, Shirley Ann, Oracle and Biometrics. Oracle Corporation: Redwood Shores CA, January 2004. p.5.

http://www.oracle.com/technology/Deploy/Security/pdf/biometrics_twp.pdf. Accessed 5 October 2005.

Also see Anil K. Jain, S.C. Dass, and K. Nandakumar, "Can Soft biometric traits assist user recognition?" (Proceedings of SPIE, Vol.54, No.4, 2004, pp.561-572,

http://www.stt.msu.edu/~sdass/papers/JainDassNandakumar_SPIE04.pdf) for scientific information on

error rates; Woodward, et al, Biometrics: A Look at Facial Recognition (Rand Corporation: Arlington VA, 2003, www.rand.org) for an in-depth examination of the challenges posed by outdoor surveillance; and

"Technology Strains to Find Menace in the Crowd," New York Times, 31 May 2004, for a brief summary of the failure of several test surveillance programs using facial recognition

(http://www.itl.nist.gov/iad/Articles/NYTimes_files/Times-05-31-04-article-face.htm.)

³⁰ Vaughan, Jessica M., Modernizing America's Welcome Mat: The Implementation of US-VISIT. Center for Immigration Studies: Washington D.C., August 2005. p.3. <http://www.cis.org/articles/2005/back905.pdf>

Accessed 4 October 2005.

³¹ "U.S. Passport Plan Draws Fire." The Globe and Mail: Toronto, 6 October 2005, p.A16.

³² Bodenheimer, David. "Technology for Border Protection: Homeland Security Funding and Priorities." Homeland Security Journal, August 2003. www.homelandsecurity.org/journal/Articles/bodenheimer.html.

p.5. Accessed 6 February 2004.

³³ Kingsbury, 2003. p.5.

³⁴ Kingsbury. 2003. pp. 5-6.

³⁵ Hurst, Lynda. "Bio-security still a fantasy: Airport screening won't work." The Toronto Star, 24 January 2004. www.thestar.com. Accessed 24 January 2004.

³⁶ Walker, 2003.

³⁷ Kingsbury, 2002. pp. 153-154.

³⁸ Jain, et al, p.2. Full results of FVC2004 are available at: <http://bias.csr.unibo.it/fvc2004/default.asp>

³⁹ Ibid., p.9 (chart), Bodenheimer, 2003, p.1.

⁴⁰ Hurst, 2004.

⁴¹ Jain, A.K., Dass, S.C., Nandakumar, K., "Can soft biometric traits assist in user recognition?" Proceedings of SPIE, Vol.54, No.4, 2004, p.562.

http://www.stt.msu.edu/~sdass/papers/JainDassNandakumar_SPIE04.pdf Accessed 5 October 2005.

⁴² Pankanti, Sharath, Salil Prabhakar, Anil Jain, "On the Individuality of Fingerprints," IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.24, No.8, August 2002. p.1010.

<http://biometrics.cse.msu.edu/cvpr230.pdf> Accessed 6 October 2005.

⁴³ Kingsbury, 2002. p.139.

⁴⁴ Goldfarb, Danielle, Thinking the Unthinkable: Security Implications and Canada's Long-Term Strategies. C.D. Howe Institute, January 2004. www.cdhowe.org/pdf/backgrounder_77.pdf. pp.1-4. Accessed 23 January 2004.

⁴⁵ Knox, Paul. The Globe and Mail. Toronto. 7 February 2004. p. A10.

⁴⁶ Strickland and Willard. 2002. p.1.

⁴⁷ Ibid., p.16.

⁴⁸ Ibid.

⁴⁹ The main programs are SEVIS (Student and Exchange Visitor Information System), CIPRIS (Coordinated Interagency Partnership Regulation), and NSEERS (National Security Entry-Exit Registration System). These new programs are meant to interact with existing programs such as USVISIT, and a number of databases. For a quick overview of the tracking issues see Nancy Kingsbury, Homeland Security: Overstay Tracking is a Key Component of Layered Defence, GAO Report #GAO-04-170T, 16 October 2003, <http://www.gao.gov/new.items/d04170t.pdf>, Jenks and Camarota for an understanding of the various programs, and Vaughan for a recent critique of the stages of implementation of the programs.

⁵⁰ A detailed study of the immigration histories of terrorists operating within the U.S. from the early 1990s to 2004 was completed by Janice L. Kephart in September 2005. Her superlative report is entitled Immigration and Terrorism: Moving Beyond the 9/11 Staff Report on Terrorist Travel. (Center for

Immigration Studies: Washington D.C.) <http://www.cis.org/articles/2005/kephart.pdf> Accessed 3 October 2005.

⁵¹ Rhodes, p.20

⁵² See The Al Qaeda Manual, a document seized in police raids in Manchester England in 2001.

<http://www.usdoj.gov/ag/trainingmanual.htm> Accessed 9 October 2005.

⁵³ Information on the perpetrators of the London bombings is available at:

<http://news.bbc.co.uk/1/hi/uk/4678837.stm>

⁵⁴ Jonas, 2004.

⁵⁵ A prime example is the diverse funding networks that many terrorist groups rely upon. The people gathering this funding are examples of 'permanent staff.' See for example ⁵⁵ Mark Basile, "Going to the Source: Why Al Qaeda's Financial Network is Likely to Withstand the Current War on Terrorist Financing." *Studies in Conflict and Terrorism*, Vol.27, 2004. London: Taylor & Francis. pp.169-188, Rohan Gunaratna, *Inside Al Qaeda: Global Network of Terror*. New York: Columbia University Press. 2002, and Napoleoni, Loretta. *Modern Jihad: Tracing the Dollars Behind the Terror Networks*. Sterling, VA: Pluto Press. 2003.

⁵⁶ Strickland and Willard. 2002, p.10.

⁵⁷ Document fraud has been pervasive in the U.S. as well as Canada. See Marti Dinerstein, *America's Identity Crisis: Document Fraud is Pervasive and Pernicious*, Washington D.C.: Center for Immigration Studies, April 2002. <http://www.cis.org/articles/2002/back302.pdf>. Accessed 3 October 2005.

⁵⁸ Goldfarb, 2004. p.4.

⁵⁹ Adamson, Rondi. *The Christian Science Monitor*. 20 January 2004.

<http://www.csmonitor.com/2004/01/20/p11-coop.htm>. Accessed 24 January 2004.

⁶⁰ Kehaulani-Goo. 2004. Also see Vaughan 2005, p.3.

⁶¹ Information on CANPASS is available at: <http://www.cbsa-asfc.gc.ca/travel/canpass/menu-e.html>

⁶² "Government plans to test biometrics at the border," *The Globe and Mail*, 17 October 2005, p.A8.

⁶³ *Securing an Open Society: Canada's National Security Policy*, April 2004. p.42. www.pco-bcp.gc.ca

For an overview of the problems with the deployment of RTID and LiveScan see the March 2004 Report of the Auditor General of Canada to the House of Commons. <http://www.oag-bvg.gc.ca/domino/reports.nsf/html/20040303ce.html> pp. 3-23 to 3-27.

⁶⁴ The entire report is available at <http://www.oag-bvg.gc.ca>

⁶⁵ Auditor General of Canada, April 2005, pp.12-14 Unless otherwise noted, all information in the following paragraph is from Chapter 3 of the April 2005 report.

⁶⁶ Auditor General of Canada, April 2005, p.3-24.

⁶⁷ This point is made directly or alluded to by numerous American commentators, some with authority and others without. For example see Jessica Vaughan's 2005 article cited in endnote 30. Vaughan continually makes reference to the fact that "Canada has a generous legal immigration system and political asylum is available to anyone who asks for it." (p.6) She emphasizes the point by quoting a former Canadian diplomat who says "Canada's the only country that I would say hasn't significantly tightened up [immigration policies]." (p.6)

⁶⁸ Auditor General of Canada, April 2005, Chapter 2, p.3

⁶⁹ Jenks, Rosemary and Steven Camarota, *Falling Behind on Security: Implementation of the Enhanced Border Security and Visa Entry Reform Act of 2002*. Center for Immigration Studies: Washington D.C. December 2003. <http://www.cis.org/articles/2003/back1903.pdf> p.8. Accessed 4 October 2005.

⁷⁰ Hite, p.2.

⁷¹ Vaughan, p.7

⁷² Information on the EZ-Pass system is available at: <http://www.ezpass.com/index.html> Information on the described problems with the system are available at: <http://www.itsa.org/ITSNEWS.NSF/0/25023442d051d52f85256bf30076dd49?OpenDocument> and <http://www.infoworld.com/articles/hn/xml/00/10/25/001025hnezpass.html> All accessed 11 October 2005.

⁷³ Drs. Kingsbury and Tomko have already been referred to numerous times in this paper. Dr. Cavoukian is Provincial Information and Privacy Commissioner for Ontario, Jennifer Stoddart is Canada's Privacy Commissioner. Information on the concerns of Cavoukian and Stoddart is available at <http://www.ipc.on.ca/> and <http://www.privcom.gc.ca/> respectively. An good example of journalistic criticism is "Biometrics: holding my body in question," by Ken Wiwa, *The Globe and Mail*, 4 January 2004, p.A15.

⁷⁴ A comprehensive public survey of attitudes in the U.S. and Canada supporting this conclusion was published in August of 2005. See "Consumer Attitudes about biometrics in ID documents." TNS/Truste Group, August 2005. http://www.truste.org/pdf/Biometrics_study.pdf Accessed 6 October 2005.

⁷⁵ Rosenzweig, Paul, Alane Kochems, and Ari Schwartz, "Biometric Technologies: Security, Legal, and Policy Implications," Legal Memorandum No. 12, June 21 2004. The Heritage Foundation: Washington D.C. p.7.

<http://www.heritage.org/Research/HomelandDefense/loader.cfm?url=/commonspot/security/getfile.cfm&PageID=65326> Accessed 6 October 2005.

⁷⁶ For a complete overview of all of the new security initiatives that Canada and the U.S. are collaborating on see the DFAIT Press release from 3 October 2003 cited in endnote 1.

⁷⁷ Kingsbury, 2002, p. 119-120. See also "U.S. passport plan draws fire," The Globe and Mail: Toronto. 6 October 2005, p.A16.

⁷⁸ "American trips north hit 26-year low," The Globe and Mail, 20 October 2005, p.B4.

Selected Bibliography

Adamson, Rondi. The Christian Science Monitor. 20 January 2004.

<http://www.csmonitor.com/2004/01/20/p11-coop.htm>.

ANSI Biometric Standards (October 2004).

http://www.biometrics.dod.mil/documents/standards/Established_Biometric_Standards_List_041007.pdf

Bement, Arden, "S 1749/HR 3525 Enhanced Border Security and Visa Entry Reform Act." Statement to the Subcommittee on Immigration Committee on the Judiciary, United States Senate. 12 April 2002.

<http://www.nist.gov/testimony/2002/abvisa.html>.

Bodenheimer, David. "Technology for Border Protection: Homeland Security Funding and Priorities."

Homeland Security Journal, August 2003. www.homelandsecurity.org/journal/Articles/bodenheimer.html.

Cavoukian, Ann, Privacy and Biometrics. September 1999.

http://www.ipc.on.ca/scripts/index.asp?action=31&N_ID=1&P_ID=11433&U_ID=0

Deniz, O., et al, "An Incremental Learning Algorithm for Face Recognition." In Tistarelli, M., et al, eds., Biometric Authentication: International ECCV Workshop, Copenhagen, Denmark, June 2002 proceedings. Springer-Verlag: Berlin. 2002.

DFAIT press release, "Governor Ridge and Deputy Prime Minister Manley Issue One Year Status Report on the Smart Border Action Plan." 3 October 2003. www.dfait-maeci.gc.ca/can-am/

Fraser, Sheila. March 2004 Report of the Auditor General of Canada to the House of Commons. Ottawa:

Public Works and Government Services Canada. [http://www.oag-](http://www.oag-bvg.gc.ca/domino/reports.nsf/html/20040303ce.html)

[bvg.gc.ca/domino/reports.nsf/html/20040303ce.html](http://www.oag-bvg.gc.ca/domino/reports.nsf/html/20040303ce.html)

_____, April 2005 Report of the Auditor General of Canada to the House of Commons, Ottawa:

Public Works and Government Services Canada. [http://www.oag-](http://www.oag-bvg.gc.ca/domino/reports.nsf/html/05menu_e.html)

[bvg.gc.ca/domino/reports.nsf/html/05menu_e.html](http://www.oag-bvg.gc.ca/domino/reports.nsf/html/05menu_e.html)

Goldfarb, Danielle, Thinking the Unthinkable: Security Implications and Canada's Long-Term Strategies. C.D. Howe Institute, January 2004. www.cdhowe.org/pdf/backgrounder_77.pdf.

Government of Canada, News Release. October 2001. http://www.ccradrc.gc.ca/newsroom/releases/2001/oct/security_e.html

Hite, Randolph C., Homeland Security: Risks Facing Key Border and Transportation Security Program Need to be Addressed. USGAO report #GAO-04-569T, 18 March 2004.
<http://www.gao.gov/new.items/d04569t.pdf>

Hurst, Lynda. "Bio-security still a fantasy: Airport screening won't work." The Toronto Star, 24 January 2004. www.thestar.com.

Jain, Anil K., Sarat C. Dass, Karthik Nandakumar, "Can Soft Biometric Traits Assist User Recognition?," Proceedings of SPIE, Vol.54, No.4, 2004. pp.561-572.
http://www.stt.msu.edu/~sdass/papers/JainDassNandakumar_SPIE04.pdf.

Jain, Anil K., Sharath Pankanti, Salil Prabhakar, Lin Hong, Arun Ross, James L. Wayman, "Biometrics: A Grand Challenge," Proceedings of International Conference on Pattern Recognition, Cambridge, UK, August 2004. <http://biometrics.cse.msu.edu/biometricsgrandchallenge.pdf>
Jonas, George, "Biometrics Won't Catch Disposable Terrorists" The National Post. 19 January 2004.
www.canada.com.

Jenks, Rosemary, and Steven Camarota, Falling Behind on Security: Implementation of the Enhanced Border Security and Visa Entry Reform Act of 2002. Center for Immigration Studies: Washington D.C. December 2003. <http://www.cis.org/articles/2003/back1903.pdf>

Kehaulani-Goo, Sara, "Security Program Collars Criminals: USVISIT Works, House Panel Told." The Washington Post, 29 January 2004

Kephart, Janice L., Immigration and Terrorism: Moving Beyond the 9/11 Staff Report on Terrorist Travel. Center for Immigration Studies: Washington D.C. September 2005.
<http://www.cis.org/articles/2005/kephart.pdf>.

Kingsbury, Nancy, "Border Security: Challenges in Implementing Technology." Testimony before the Subcom. On Terrorism, Technology, and Homeland Security, 12 March 2003. USGAO report #GAO-03-546T <http://www.gao.gov/new.items/d03546t.pdf>.

Kingsbury, Nancy, Technology Assessment: Using Biometrics for Border Security. United States General Accounting Office (USGAO), report #GAO-03-174, November 2002.
<http://www.gao.gov/new.items/d03174.pdf>

Knox, Paul. The Globe and Mail. Toronto. 7 February 2004. p. A10.

NIST press release. "NIST Supports Multiple Biometrics for Border Security." 18 February 2003.
<http://govtsecurity.securitysolutions.com/microsites/newsarticle>.

Pankanti, Sharath, Salil Prabhakar, Anil K. Jain, "On the Individuality of Fingerprints," IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.24, No.8, August 2002, pp.1010-1025.
<http://biometrics.cse.msu.edu/cupr230.pdf>.

Privy Council Office of Canada. Securing an Open Society: Canada's National Security Policy, April 2004. www.pco-bcp.gc.ca

Rhodes, Keith A., Information Security: Challenges in Using Biometrics. USGAO report #GAO-03-1173T.
<http://www.gao.gov/new.items/d031137T.pdf>

Rosenzweig, Paul, Alane Kochems, and Ari Schwartz, "Biometric Technologies: Security, Legal, and Policy Implications," Legal Memorandum No. 12, June 21 2004. The Heritage Foundation: Washington D.C. p.7.

<http://www.heritage.org/Research/HomelandDefense/loader.cfm?url=/commonspot/security/getfile.cfm&PageID=65326>

Stern, Shirley Ann, Oracle and Biometrics. Oracle Corporation: Redwood Shores CA, January 2004.
http://www.oracle.com/technology/deployment/security/pdf/biometrics_twp.pdf

Strickland, Lee and Jennifer Willard, "Reengineering the Immigration System: A Case for Data Mining and Information Assurance to Enhance Homeland Security." Homeland Security Journal, October 2002.
<http://www.homelandsecurity.org/journal/Articles/Strickland.html>.

Tomko, George, "Biometrics as a Privacy-Enhancing Technology: Friend or Foe of Privacy?" Speech given 15 September 1998. www.dss.state.ct.us/digital/tomko.htm.

Vaughan, Jessica M., America's New Welcome Mat: A Look at the Goals and Challenges of the US-VISIT Program. Center for Immigration Studies: Washington D.C. 4 March 2004.
<http://www.cis.org/articles/2004/jessicatestimony030404.html>.

_____, Modernizing America's Welcome Mat: The Implementation of US-VISIT. Center for Immigration Studies: Washington D.C. August 2005. <http://www.cis.org/articles/2005/back905.pdf>

Walker, Richard, "Security: Biometrics Gains a Foothold" 5 May 2003. <http://www.gcn.com/cgi-bin/udt/im.display> (Post-Newsweek Media Inc.)

Woodward, John D., Christopher Horn, Julius Gatune, Aryn Thomas, Biometrics: A Look at Facial Recognition. Rand Corporation: Arlington VA, 2003. <http://www.rand.org>

Yi, Juneho, et al, "Face Recognition Based on ICA Combined with FLD." In Tistarelli, M., et al, eds., Biometric Authentication: International ECCV Workshop, Copenhagen, Denmark, June 2002 proceedings. Springer-Verlag: Berlin. 2002.