PROTECT AMERICA BY BEING UNIQUE: HOW CHANGES IN BIOMETRIC DATA COLLECTION PROCEDURES CAN IMPROVE US-VISIT

INTRODUCTION

Since 2004, the Department of Homeland Security (“DHS”) has used biometric data technology to identify virtually all foreign citizens entering the United States.\(^1\) United States Visitor and Immigrant Status Indicator Technology,\(^2\) commonly referred to as “US-VISIT,” utilizes fingerprint scanning and facial photographs to confirm the identities of foreign visitors between the ages of 14 and 79.\(^3\) Demonstrating the magnitude of the program, US-VISIT identifies about 30,000 individuals for the U.S. Department of State and 100,000 individuals for U.S. Customs and Border Protection (“CBP”) each day.\(^4\)

As this note will discuss, US-VISIT has achieved considerable success in using biometric identification technology to meet U.S. security objectives,\(^5\) but falls short of its full potential.\(^6\) While DHS has


\(^5\) See id. at 2 (providing specific examples of the use of biometric data to uncover true identity and criminal history of travelers through U.S. ports of entry).

\(^6\) See e.g., DIEM NGUYEN & JENA BAKER MCNEILL, HERITAGE FOUND., BIOMETRIC EXIT PROGRAM SHOWS NEED FOR NEW STRATEGY TO REDUCE VISA
implemented effective procedures to capture the biometric data of those entering the country, it has not yet executed a plan to collect the biometric data of those leaving it.\textsuperscript{7} If biometric exit-data were collected, immigration officials could instantly identify those aliens still present in the United States in violation of the terms of their visas.\textsuperscript{8}

Realizing the benefits of collecting this information, Congress mandated in 2007 that DHS develop a system to collect biometric exit-data by June of 2009,\textsuperscript{9} but doing so has proven problematic.\textsuperscript{10} Indeed, DHS notes that the infrastructure, land, and resources necessary to construct a collection system at the country’s points of exit that mirror those at the points of entry are impracticable.\textsuperscript{11} According to the Heritage Foundation, exit collection systems could cost DHS between $3.1 billion and $6.4 billion over the next ten years.\textsuperscript{12} To put this cost in perspective, DHS has spent only $1.3 billion on the implementation of an entry-data collection system. In light of these staggering costs, some have even questioned the value of obtaining biometric exit-data.\textsuperscript{13}

Yet, are there alternative solutions that would allow for the collection of exit-data without requiring DHS to absorb this unreasonable expense? This Note advocates for increased security cooperation with border countries such as Canada. In so doing, significant cost savings could be realized if the United States were to take advantage of the infrastructure already in place at the respective borders. Additionally, this Note reviews biometric technologies already employed at the borders of foreign countries that could be adopted by the United States to mitigate some of the impracticability cited by DHS.

Part I of this note will examine the current implementation of biometric identification technologies used by immigration officials in

\textsuperscript{7} BIOMETRICS AND YOU, supra note 2, at 3; see generally NGUYEN & MCNEILL, supra note 6 (providing background information about proposed exit programs).

\textsuperscript{8} See NGUYEN & McNEILL, supra note 6, at 2.


\textsuperscript{12} NGUYEN & McNEILL, supra note 6, at 4.

\textsuperscript{13} Id.
the United States. Part II will identify and discuss possible programs with Canada that could mitigate the costs associated with the implementation of an exit-data collection system. It will also identify technological advances and future collection procedures that could improve the success of the program.

I. U.S. IMMIGRATION’S IMPLEMENTATION OF BIOMETRIC IDENTIFICATION TECHNOLOGY

A. History of Federal Legislation Calling for Biometric Data Collection

In an attempt to “strengthen and tighten the immigration law” and “improve border control,”14 the U.S. Congress passed the Illegal Immigration Reform and Immigrant Responsibility Act (“IIRIRA”) in 1996.15 IIRIRA required U.S. immigration officials to implement an “automated entry and exit control system” to “collect a record of departure for every alien…and match the records of departure with the record of the alien’s arrival in the United States.”16 In response to this legislation, Immigration and Naturalization Services (“Legacy INS”)17 created the National Automated Immigration Lookout System (“NAILS”).18

16 Id. at §110.
Legacy INS, in conjunction with the State Department and customs authorities, used NAILS to identify and screen all foreigners seeking entry into the United States.\(^\text{19}\) The system relied on a database containing biographical information for individuals which could be cross-referenced during visa application review procedures and at immigration points of entry.\(^\text{20}\) Unfortunately, foreign travelers could evade NAILS identity detection easily by using false names and fraudulent documentation.\(^\text{21}\)

After the events of September 11, 2001, Congressional leaders became increasingly critical of the biographical nature of the NAILS database because of the ease with which foreigners could bypass detection.\(^\text{22}\) To address these deficiencies, the Congress passed a number of national security initiatives, including the Intelligence Reform and Terrorism Prevention Act of 2004.\(^\text{23}\) Its purpose was to “attack document fraud which aids terrorists in entering the United States.”\(^\text{24}\) A key component of this legislation was the requirement that the newly-created DHS incorporate biometric identification technology into the immigration process and form an integrated system to track entry and exit-data for foreign visitors.\(^\text{25}\)

To comply with the new biometric requirement, DHS created the National Security Entry-Exit Registration System (“NSEERS”).\(^\text{26}\) NSEERS required foreign visitors from 23 targeted countries,\(^\text{27}\) as

---

19 Id.
20 Id.
21 Id.
22 Id. ("[NAILS] is effective only if an applicant uses a name that has been entered into the database; false names, supported by fraudulent documentation, can help an individual to evade identification….").
23 See Krutschik, supra note 14, at 465 (discussing the legislative response to 9/11).
24 Id. at 465-66.
27 Targeted countries included: Afghanistan, Bangladesh, Egypt, Eritrea, Indonesia, Iran, Iraq, Jordan, Kuwait, Lebanon, Libya, Morocco, North Korea, Oman, Pakistan, Qatar, Saudi Arabia, Somalia, Sudan, Syria, Tunisia, United Arab Emirates, and Yemen. David S. Ortiz et al., Revisiting US-Visit: U.S. Immigration
well as travelers DHS identified as “being of interest,” to submit to questioning and biometric registration upon entry to the United States. Questions asked during the interviews included the individual’s email address, details about personal contacts and family members, bank accounts, credit card numbers, employer addresses, and school addresses. Upon learning of the countries to be targeted, commentators noted that the program “patently target[ed] Muslims and Arabs in America.”

Compounding concerns of racial profiling, NSEERS also included a special “call-in registration” component. This aspect of the program called for all travelers from 25 countries that entered the United States on a temporary visa to report to a DHS facility for biometric registration. International human rights groups described this retroactive special registration as discriminatory and violations of international law, as specific populations of immigrants were targeted including, for example, Pakistanis, Saudi Arabians, Bangladeshis and Egyptians. While NSEERS stirred political controversy in Congress and resulted in mass protests by ethnic groups and civil liberties advocates, it resulted in the federal government’s first attempts to incorporate biometric information into the immigration process by requiring fingerprints and photographs of those registered under the program.

Fingerprint identification technology analyzes the patterns of minute ridges and furrows of skin present on the fingers and toes of hu-
It is one of the most reliable techniques available to immigration enforcement officials for one simple fact: no person has ever been found to possess the same pattern of ridges and furrows as another. Furthermore, the unique characteristics of an individual’s fingerprints do not change with time.

While other biometric identification techniques exist, fingerprint technology is unique in that immigration officials already have a large database of records upon which they may draw. The United States Government Accountability Office notes that fingerprint technology is the optimal biometric identification technology because it can leverage existing DHS and Federal Bureau of Investigation (“FBI”) identification databases. The FBI has pooled and archived the fingerprint records from U.S. law enforcement agencies since the 1920s and its Integrated Automated Fingerprint Identification System is now the largest biometric database in the world, with over 400 million prints.

DHS later expanded NSEERS to include biometric registration of all foreign visitors to the United States. By expanding the program to all foreigners, NSEERS no longer targeted certain ethnicities or geographic regions to the behest of many human rights organizations. This comprehensive program developed into what is now US-VISIT, which is led by a director, who reports to the Deputy Secretary for Homeland Security. The program office is generally respon-

---

36 Id. at 3.
37 U.S. Gov’t Accountability Office, GAO-03-174, TECHNOLOGY ASSESSMENT: USING BIOMETRICS FOR BORDER SECURITY 139 (2002) (“Scientific studies in the mid-1800s established the persistence of friction ridge patterns on human fingers, beginning in the embryonic stage and extending throughout life, except for accidental damage.”).
38 See U.S. Gov’t Accountability Office, GAO-08-361, HOMELAND SECURITY: STRATEGIC SOLUTION FOR US-VISIT PROGRAM NEEDS TO BE BETTER DEFINED, JUSTIFIED, AND COORDINATED 31 (2008) (discussing the various fingerprint databases upon which the US-VISIT program may draw).
39 Id.
42 See Martin, supra note 18, at 335 (providing background information about the creation of US-VISIT).
sible for the “acquisition, deployment, operation, and sustainment of US-VISIT.”

B. The Current US-VISIT Biometric Data Collection Process

Most foreign visitors between the ages of 14 and 79 follow US-VISIT immigration procedures when travelling to the United States. US-VISIT and the immigration process include three distinct stages: (1) pre-travel visa issuance where required, (2) biometric data collection upon the traveler’s entry to the United States, and (3) biographic data collection upon the traveler’s departure from the United States.

1. Pre-Travel Visa Issuance Process

The United States does not generally require a visa for travelers from 27 countries participating in its Visa Waiver Program. Travelers from other countries, however, must obtain a visa to enter the country. A visa permits the visitor to travel to U.S. points of entry, such as airports, seaports and land border crossings, and request entry to the country. However, the United States maintains the right to refuse entry to the country even if the traveler has a visa. To obtain a visa, travelers must visit a U.S. consular office or embassy before

---

44 Id.
46 See, e.g., BIOMETRICS AND YOU, supra note 2, at 1-3.
47 Participating countries include Andorra, Austria, Australia, Belgium, Brunei, Denmark, Finland, France, Germany, Iceland, Ireland, Italy, Japan, Liechtenstein, Luxembourg, Monaco, the Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovenia, Spain, Sweden, Switzerland, and the United Kingdom.
49 Id. at 2. A visa is still required for travelers from Visa Waiver Program countries if the traveler “intend[s] to stay longer than 90 days, intend[s] to travel to the United States for a reason other than business or tourism, ha[s] ever been arrested even if not convicted, ha[s] a criminal record, ha[s] a serious, communicable disease (including HIV), ha[s] been refused entry to the United States on a previous occasion, ha[s] been deported from the United States, ha[s] previously overstayed the 90 days [on a previous trip to the United States], or [is] a child included on [a] parent’s passport.”Id. at n.2.
50 Id.
51 See id. (“A visa allows you to travel to the United States as far as the port of entry (airport, seaport or land border crossing), where the Customs and Border Protection (CBP) officer has the authority to permit you to enter the United States.”).
arriving in the United States. There, a representative from the U.S. Department of State reviews the traveler’s visa application and collects the traveler’s biometric data, including a ten-finger fingerprint scan and a digital photograph. The biometric data is then saved and cross-referenced with all other entries in the US-VISIT database.

2. Data Collection Upon Entry to the United States

When travelling to the United States by ship or airplane, an airline or cruise representative provides the traveler with an entry form that must be completed prior to arrival. Travelers from countries in the United States’ Visa Waiver Program complete a Form I-94W, while travelers from other countries complete a Form I-94. Upon disembarking from the airplane or ship, a CBP officer interviews the traveler and reviews the requisite travel documentation as well as the I-94 or I-94W form. The CBP officer scans all ten of the traveler’s fingerprints using the US-VISIT’s inkless fingerprinting technology and takes a digital photograph of the traveler’s face. US-VISIT saves the biometric data and cross-references it against other entries in its database, including the fingerprint data taken during the visa application interview. In the event that the database matches the scan to the correct visa application, the CBP officer will permit the traveler to enter the country. Land border crossings follow modified protocols depending on the border location and citizenship of those seeking entry.

52 See BIOMETRICS AND YOU, supra note 2, at 1 (directing travelers to contact the “closest U.S. visa-issuing post”).
53 Id. In addition to the visa application, foreign travelers may also have to submit certain forms and supporting documents. See generally U.S. DEP’T OF STATE, TYPES OF VISAS FOR TEMPORARY VISITORS, http://travel.state.gov/visa/temp/types/types_1286.html# (last visited Mar. 5, 2011).
54 BIOMETRICS AND YOU, supra note 2, at 1.
56 BIOMETRICS AND YOU, supra note 2, at 1.
57 Id.
58 Id.
59 Id.
60 Miller, supra note 55, at 206 (describing how CBP officers cross-reference fingerprints in an effort to reveal possible “red flags” before the traveler enters the United States).
61 BIOMETRICS AND YOU 2, supra note 2, at 2.
Mexico-U.S. border, all travelers who are not citizens of Mexico or the United States must follow the same process as travelers arriving at airports and seaports. Foreign travelers must complete a Form I-94 as well as have their biometric data recorded per US-VISIT protocol. Mexican citizens who plan to stay in the United States more than thirty days or who are travelling away from the border also follow these requirements. Mexican citizens who plan to stay less than thirty days and who plan to remain in the “border zone,” however, may be issued a Border Crossing Card. This card allows them to cross the border without completing a Form I-94 or having to provide biometric data for the US-VISIT program. On the other hand, at the Canada-U.S. border, most Canadians are exempt from the US-VISIT program. All other travelers who are not Canadian or United States citizens must submit to US-VISIT data collection procedures at the border.

3. Data Collection Upon Departure from the United States

When departing from the United States by airplane or ship, travelers must return their I-94 or I-94W form to the appropriate airline or ship representative, which completes the immigration process. Congress mandated that DHS implement a nationwide system for collecting biometric exit-data for departing travelers by 2009, but such a


U.S.-MEXICO LAND BORDER, supra note 62.

Id.

Id.

Id.


U.S.-MEXICO LAND BORDER, supra note 62.

Id. However, if the traveler uses a Border Crossing Card and the immigration official asks for a secondary inspection, that traveler becomes subject to US-VISIT’s requirements. Id.

U.S.-CANADA BORDER, supra note 62. Canadians are subject to the US-VISIT program, however, if they are: (1) dual-citizens and are travelling under their non-Canadian passport, or (2) using a U.S. treaty trader (E) or a fiancé (K) nonimmigrant visa. Id.

Id. (“US-VISIT currently applies to most visitors (with limited exemptions) entering the United States, regardless of country of origin or whether they are traveling on a visa.”).

BIOMETRICS AND YOU, supra note 2, at 3.

CURRENT U.S. BIOMETRIC EXIT PROCEDURES, supra note 3, at 3.
process has not yet been executed. Creating an exit-data collection system is challenging because most United States “airports, railway stations, and border posts do not have physical space allocated for exit-control activities.” Thus, the cost and space necessary to implement this kind of infrastructure makes exit-data collection impracticable in many locations.

Nevertheless, two biometric exit-data collection pilot programs were commenced in May of 2009. Specifically, U.S. Transportation Security Administration ("TSA") officers began collecting biometric exit-data from non-citizens at security checkpoints at Atlanta’s Hartsfeld-Jackson Atlanta International Airport. Customs and Border Protection officials performed similar procedures at Detroit’s Wayne County Airport. The intent was that these pilot programs would allow for the development of nationwide biometric exit-data collection procedures. As noted by DHS Secretary Janet Napolitano during the testing, “[t]he pilot programs in Atlanta and Detroit will help [the United States to] determine and develop standard procedures for use at airports across the country to expedite legitimate travel and enhance our nation’s security.” During these pilot programs, TSA agents still collected departure Forms I-94 and I-94W. Following the pilot program, US-VISIT installed exit-data collection kiosks in thirteen airports and three seaports. The kiosks are located in a secure part of the airport and are monitored by U.S. immigration officials.

---

73 BIOMETRICS AND YOU, supra note 2, at 3.
74 ORTIZ, supra note 27, at 13.
75 Id.
77 Id.
78 Id.
79 Id. CBP and TSA used different techniques for identifying which passengers required biometric scanning. CBP used temporary signs at the gate directing visitors to collection points. TSA checked boarding passes and directed non-U.S. travelers to a secondary inspection zone. The pilots were designed to identify the most accurate protocol for exit-data collection. See U.S. DEP’T. OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE UNITED STATES VISITOR AND IMMIGRANT STATUS INDICATOR TECHNOLOGY (US-VISIT) PROGRAM, COMPREHENSIVE EXIT PROGRAM: AIR EXIT PILOT 4 (2009), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_air_exit.pdf
81 Id.
82 US-VISIT installed biometric collection kiosks at airports in Baltimore, Dallas, Chicago, Denver, Detroit, Fort Lauderdale-Hollywood, Atlanta, Newark,
The U.S. Government Accountability Office ("GAO") notes, however, that one of the primary obstacles to completing an exit-data collection program is the additional infrastructure requirements at land border crossings.\textsuperscript{84} DHS estimates that implementing such a system would cost approximately $3 billion,\textsuperscript{85} but one policy group has estimated that the cost would be somewhere between $3.1 billion and $6.4 billion.\textsuperscript{86} Furthermore, the implementation plans under consideration by DHS would require a collection protocol that would mirror US-VISIT entry procedures.\textsuperscript{87} U.S. border officials would need to review the travel documents for each exiting traveler and compare that information to the traveler’s biometric identity.\textsuperscript{88} Traffic congestion in exit lanes would increase dramatically because of the need for each vehicle to stop for processing—an outcome DHS officials view as unacceptable.\textsuperscript{89} In some cases, an exit system that mirrors US-VISIT entry procedures would be unfeasible, specifically at urban border crossings where land constraints exist.\textsuperscript{90} While DHS has tested interim procedures for tracking non-biometric exit-data, it estimated that the technological advancements necessary for a feasible border-exit implementation would not be available for another five to ten years.\textsuperscript{91}
C. Purposes of the US-VISIT program

US-VISIT’s slogan, “Keeping America’s Doors Open and Our Nation Secure,” emphasizes the multi-faceted purpose of the program. DHS has identified four principal goals for implementing a biometric tracking system for foreign visitors: (1) enhancing the security of U.S. citizens and visitors; (2) expediting legitimate travel and trade; (3) ensuring the integrity of the U.S. immigration system; and (4) safeguarding the personal privacy of visitors to the United States.

1. Enhancing Security for U.S. Citizens and Visitors

While immigration policies and procedures cannot prevent terrorist acts, “they are key ingredients of the effort to combat terrorism” and related U.S. national security interests. DHS has recently stated that “[b]iometrics—unique physical characteristics, such as fingerprints, that can be used for automated recognition—form the foundation of US-VISIT’s identification services because they are reliable, convenient and virtually impossible to forge.” Travelers can easily change names and dates of birth on travel documentation, but biometrics are unique for each individual. Prior to US-VISIT, immigration officials relied primarily upon paper-based documents that were susceptible to fraud or alteration. Incorporating biometric data into the immigration process significantly increases the ability to detect fraudulent and altered travel documents. Biometric data also allows officials to verify the identity of individuals applying for visas with a

---

93 BIOMETRICS AND YOU, supra note 2, at 1.
94 Martin, supra note 18, at 329.
95 ENHANCING SECURITY THROUGH BIOMETRIC IDENTIFICATION, supra note 4, at 3.
96 NEW BIOMETRIC TECHNOLOGY IMPROVES SECURITY, supra note 92, at 2 (“The United States collects biometrics because unlike names and dates of birth, which can be changed, biometrics are unique and almost impossible to forge.”).
97 ENHANCING SECURITY THROUGH BIOMETRIC IDENTIFICATION, supra note 4, at 2.
98 Id. To illustrate this point, DHS provides anecdotal “success stories” where biometric data collection helped uncover fraudulent documents, which may not have been revealed prior to US-VISIT’s implementation. Id.
greater veracity, where before they needed to rely primarily on biographic background information.\textsuperscript{99}

The ability to digitize biometric data also allows for increased cooperation between agencies and countries and offers inter-agency access to vital information\textsuperscript{100} because US-VISIT provides a single source of biometric data for “dangerous people.”\textsuperscript{101} Examples of collaboration through US-VISIT are numerous. The Department of State uses US-VISIT to gather the identities of visa applicants at consulates and embassies.\textsuperscript{102} CBP collects biometric data at United States points of entry and uses that information to confirm the identity of travelers attempting to enter the United States.\textsuperscript{103} CBP also uses US-VISIT to track the identities of those illegal immigrants apprehended at the border.\textsuperscript{104} Citizenship & Immigration Services uses US-VISIT to verify the identity of those applying for immigration benefits like asylum and refugee status.\textsuperscript{105} Immigration and Customs Enforcement (“ICE”) uses US-VISIT’s database to track individuals who have overstayed the time limit on their visas.\textsuperscript{106} The U.S. Coast Guard (“USCG”) identifies individuals apprehended during illegal migrant interdiction missions with US-VISIT.\textsuperscript{107} The Department of Defense and the Intelligence Community are able to identify terror suspects by cross-referencing biometric information collected at known terrorist safe houses or training camps with information in the US-VISIT database.\textsuperscript{108} The Department of Justice, through the FBI, uses US-VISIT to assist state and local law enforcement officers during investigations.\textsuperscript{109} Indeed, US-VISIT possesses a dedicated Biometric Support Center that provides forensic analysis and identification assistance for federal, state, and local agency investigations twenty-four hours a day, seven days a week.\textsuperscript{110}

\textsuperscript{99} Id. (noting that the near-impossibility of forging biometric data increases its veracity).
\textsuperscript{100} Id. (explaining that after US-VISIT there is “[b]etter coordination with other agencies; [because there is] a single source for biometrics-based information on dangerous people” and on a global scale, “[c]ountries are adopting similar standards to stop criminals, immigration violators and known or suspected terrorists”).
\textsuperscript{101} Id.
\textsuperscript{102} Id. at 4.
\textsuperscript{103} Id.
\textsuperscript{104} Id.
\textsuperscript{105} Id.
\textsuperscript{106} Id.
\textsuperscript{107} Id.
\textsuperscript{108} Id.
\textsuperscript{109} Id.
\textsuperscript{110} Id.
tion by centralizing the location of the data collected by each of these individual agencies.\footnote{111}{Id. Because close allies to the United States are also implementing similar programs with like standards, immigration officials have access to biometric data across the globe. This allows for identification of potentially “dangerous people” through international collaboration. Id.}

Although the program is relatively new, DHS already has advertised success stories demonstrating US-VISIT’s ability to increase security. For example, when a foreign national arrived at New York’s John F. Kennedy International Airport, all of his immigration and visa documentation appeared to be in order.\footnote{112}{Id. at 2.} On paper, he had no history of criminal or immigration violations. When U.S. immigration officials scanned the man’s fingerprints, however, they discovered that the visa documentation was for the man’s twin brother. The man at the airport had previously been arrested for illegally taking photographs of a U.S. military base and thus, CBP officials refused entry.\footnote{113}{Id.}

In another case, a foreign national applied for U.S. asylum using an alias and an incorrect date of birth to disguise his identity.\footnote{114}{Id.} After immigration officials referenced his fingerprints with the US-VISIT database, “his biometrics revealed an extensive criminal record, including charges for rape, assault, and an outstanding warrant for kidnapping.”\footnote{115}{Id.} Immigration officials alerted law enforcement, who arrested the man.\footnote{116}{Id.}

In an example of international cooperation, a man was detained in the United Kingdom after attempting to apply for asylum illegally.\footnote{117}{Id.} When the man applied for asylum, the United Kingdom cross-referenced his fingerprints with the US-VISIT database, and discovered that the man had previously traveled to the United States under a false name, and was attempting to hide his true identity in his asylum application. The United Kingdom learned that the man was wanted on rape charges in Australia and promptly deported him to face criminal proceedings in that country.\footnote{118}{Id.}

The most compelling demonstration of US-VISIT effectiveness, however, may be the USCG’s use of the biometric data technology in the seas around the Caribbean.\footnote{119}{Id. at 5.} During one illegal migrant interdiction mission, the USCG detained ten illegal migrants attempting to
enter Puerto Rico by sea. After tracking the identities of the individuals through the US-VISIT database, USCG discovered that two of the individuals had illegally entered the United States on a prior occasion, and were believed to be part of a human trafficking criminal enterprise. The USCG detained the two and brought them ashore for prosecution. USCG reports that since its implementation of biometric collection procedures in accordance with the US-VISIT program, “prosecutions of repeat offenders have increased dramatically and illegal migration has dropped by 75 percent in the area where the [US-VISIT] technology is being used.”

Statistics also suggest that the US-VISIT program appears to be providing tangible assistance for immigration officials. In Fiscal Year 2007, US-VISIT identified 25,552 individuals applying for visas at consular offices and another 11,685 individuals at United States ports of entry who were on biometric watch lists. During that year, US-VISIT also provided ICE with the names of 12,000 foreign travelers who had overstayed their allotted time in the United States, 273 of whom ICE ultimately detained. Furthermore, US-VISIT flagged and identified 11,246 individuals who entered the United States and subsequently committed a crime during their stays. A DHS official has indicated that at least two of the nineteen terrorist hijackers responsible for the September 11, 2001 attacks may have been stopped by the US-VISIT program and denied entry to the country. Overall, since the program’s inception in 2004, over 1,350 individuals with immigration violations and criminal records have been stopped from entering the United States.

2. Promoting Legitimate Travel and Trade

While US-VISIT’s primary purpose is to promote security, DHS recognizes an equally important objective of promoting the speed and efficiency of legitimate travel and trade. Because biometric data is

---

120 Id.
121 Id.
122 Id.
123 Id.
124 See Brazil to Fingerprint US Citizens, BBC NEWS (Dec. 31, 2003, 8:14 AM), http://news.bbc.co.uk/2/hi/americas/3358627.stm; see also THE 9/11 COMMISSION REPORT, supra note 18, at 564 n. 33 (“Two hijackers could have been denied admission at the port of entry based on violations of immigration rules governing terms of admission.”).
125 Miller, supra note 55, at 208 (footnote omitted).
126 BIOMETRICS AND YOU, supra note 2, at 1.
unique, US-VISIT can facilitate travel for those legitimate travelers who lose their passports or travel documentation.  For instance, Interpol reports indicate that 6.7 million passports have been lost or stolen since 2001, 2.8 million of which were from the United States’ Visa Waiver Program countries. To this point, US-VISIT and its use of biometric data speeds the re-issuance of travel documentation for U.S. citizens, promoting efficiency in the event a traveler loses his or her passport.

Officials may also use US-VISIT to facilitate the visa issuance process. In 2000, more than 10 million foreign citizens applied for visas to enter the United States. Prior to US-VISIT, critics claimed that visa officers were too cautious and denied visas to too many applicants with legitimate travel reasons. State department officials had previously reviewed visa applications using NAILS, a name-based database, but this proved problematic because travelers using a false name and fraudulent travel documentation could easily evade the system. Ultimately, tracking names with fingerprints and passports with biometric identifiers significantly reduced the need for extensive background checks for most visa applications.

US-VISIT is also taking proactive steps to reduce the burden it places on travelers entering the United States. In November of 2007, DHS began upgrading most fingerprint scanners used at United States points of entry from two-finger technology to ten-finger technology. The upgrades were complete by December of 2008 and took place at all major points of entry. Initially, some critics worried that scanning more fingers would increase wait times and immigration

127 See NEW BIOMETRIC TECHNOLOGY IMPROVES SECURITY, supra note 92, at 2 (“By using biometrics to establish and verify travelers’ identities, we are making international travel more convenient, predictable and secure for legitimate visitors, but difficult, unpredictable and intimidating for criminals, immigration violators and those who want to do harm to the United States.”).
128 Id.
129 Id.
130 Martin, supra note 18, at 331.
131 Id.
132 Id. at 332.
133 See also discussion supra Part I.A.
134 Miller, supra note 55, at 207.
136 Id. (noting that most foreign visitors entering the United States experience this new scanning technology).
lines, but DHS officials note that the new scanners actually decrease the time it takes to identify an individual. In fact, border checks are now estimated to take less than one minute to complete. This increase in efficiency is due to the fact that the additional fingerprints provide more data to reference with the US-VISIT biometric database, allowing the system to find a match faster and with greater accuracy. This increase in accuracy should also substantially decrease the number of legitimate travelers who are mistakenly identified and taken for questioning, allowing for a more efficient immigration process. GAO recently reported that immigration officers at every U.S. point of entry surveyed agreed that US-VISIT improved their ability to identify and process travelers quickly.

To ensure that immigration procedures are easy and predictable for legitimate travelers, DHS has also engaged in an aggressive media campaign to educate visitors about the new biometric collection procedures. DHS has made presentations at over 500 events in 26 countries around the world, created educational materials in 15 languages, and has worked with “government and private sector partners to ensure widespread reach to travelers around the world.” DHS notes that these efforts are designed to improve efficiency in travel and avoid confusion that may arise for foreign travelers.

3. Ensuring the Integrity of the U.S. Immigration System

Prior to US-VISIT, the United States had difficulty regulating the free circulation of dangerous people after they entered the country. For example, at least sixteen of the September 11\textsuperscript{th} hijackers entered the United States legally with valid visas, but immigration officials did not track their activities once the terrorists entered the country.
Had immigration officials monitored the hijackers’ activities subsequent to their entry into the United States, officials would have discovered that some were in violation of the terms of their visas. For instance, one hijacker was granted entry on a student visa, but never showed up to the University to which he was admitted. Beyond the events of 9/11, problems with the improper entry of foreigners into the United States are widespread. In 2000, there were an estimated 8.5 million unauthorized foreigners in the United States. While most do not pose a security threat, this pervasive nature of illegal immigration hampers officials’ efforts to identify true security threats. Current mechanisms used by immigration officials to identify unauthorized entry or violations of visa terms are unable to correct the problem and thus, the need for a better system is apparent.

Generally, visitors who violate their visa’s approved length of stay in the United States can be tracked using the exit-data collected from the Form I-94 that is returned to immigration officials when leaving the country. Unfortunately, compliance with collection protocols is spotty and many visitors exiting the United States through land border-crossings do not return their forms. This limits the effectiveness of the present tracking system that DHS can use to identify visa violators. Furthermore, I-94 forms are not very effective at tracking the departures of specific individuals because they are completed by hand, which means that U.S. immigration officials must enter the data into a computer manually, slowing the identification of violators. As noted by a senior immigration official in testimony given before the Senate Committee on Finance, the use of biometric data in entry-exit tracking systems would allow immigration officials to determine instantly whether a particular alien has overstayed his or her visa, which would be a considerable improvement over the current system.

148 Id.

149 Id. at 337.

150 Id. at 336-37 (noting, for example, that “[a]lthough...unauthorized workers do not themselves pose a security threat, tolerance of their entry and presence in the country hampers efforts to close the back door of illegal migration—a backdoor that terrorists can too easily exploit for their own purposes”).

151 Id. at 333.

152 Id.

153 Id.

4. Safeguarding Personal Privacy of Visitors

Because the collection of biometric data involves highly personal information unique to an individual, there is the obvious concern that if not regulated, this information could be used or shared in an improper way. DHS maintains that it only uses the biometric data for the purposes for which it was collected, and as authorized or mandated by law. To ensure that this goal is met, the US-VISIT program has created an officer position responsible for maintaining privacy and confidentiality. Further, in the event that a traveler believes that the information in US-VISIT’s database is incorrect, DHS provides multiple avenues for correcting the mistake. For example, foreign travelers may make inquiries into their personal data or immigration-related screening issues through the Traveler Redress Inquiry Program (“TRIP”). Individuals can initiate inquiries through an interactive website, by sending an email to US-VISIT’s Privacy Officer, or by mailing a hard-copy of all travel documentation to US-VISIT’s office at DHS headquarters in Washington, D.C.

There have been some recent concerns, however, about the integrity of the privacy safeguards in place. In one such complaint filed under the Freedom of Information Act, a journalist sought information from CBP regarding the unexpected malfunction of US-VISIT computers on August 18, 2005. According to a spokesperson for the DHS, a system shutdown occurred due to a virus that impacted computer systems in New York, San Francisco, Miami, Los Angeles, Houston, Dallas, and Laredo, Texas. DHS later reported that US-VISIT computers occasionally malfunction.

US-VISIT’s privacy policy has also been subject to criticism from foreign nationals. In another Freedom of Information Act complaint against DHS, a member of the European Union’s parliament was con-

---

155 See ENHANCING SECURITY THROUGH BIOMETRIC IDENTIFICATION, supra note 4, at 6 (explaining the US-VISIT’s privacy policy).
156 NEW BIOMETRIC TECHNOLOGY IMPROVES SECURITY, supra note 92, at 3 (noting that “US-VISIT has a dedicated privacy officer, who is responsible not only for ensuring compliance with privacy laws and procedures, but also for creating a culture within the program where privacy is inherently valued, treated as a fundamental right and obligation, and fully considered in US-VISIT’s planning and development processes”).
157 Id. at 3-4.
158 Id. at 3.
159 Id. at 3-4.
161 Id. at *2.
162 Id.
cerned with a notice published by DHS stating that it had instituted a program called the Automated Targeting System. This was a method of data-mining used by various databases—including US-VISIT—to create risk assessments for travelers entering the United States. The parliament member alleged that this treatment of passenger data was a violation of European Union citizens’ “fundamental rights.” These allegations echoed domestic statements made by the American Civil Liberties Union (“ACLU”), claiming that the U.S. terror watch lists that feed these systems are “bloated and full of inaccuracy” due to the ACLU’s inability to ascertain the criteria for adding or removing an individual from these lists. Going forward, DHS hopes to resolve these issues through its latest privacy initiatives, including its TRIP grievance process.

II. BIOMETRIC EXIT-DATA COLLECTION OPPORTUNITIES ARE AVAILABLE TO IMPROVE THE US-VISIT SECURITY INITIATIVE’S SUCCESS

As previously discussed, US-VISIT’s true potential lies in obtaining biometric data from those exiting the country. While operational realities and resource restrictions limit the ability of U.S. immigration officials to obtain this exit-data in the same manner as when foreigners enter the country, creative approaches to data collection procedures could allow for the collection of this information. First, sharing border-crossing infrastructure and staffing with Canada could dramatically improve US-VISIT’s exit-data collection capabilities. Second, there are opportunities for foreign visitors’ biometric data to be collected upon entry to Canada in accordance with DHS’s goal of pushing immigration procedures away from the United States’ physical border. Finally, US-VISIT could incorporate new forms of border enforcement identification technologies, such as RFID tagging and iris recognition software.

---

164 Id.
165 Id.
166 Jun Hongo, Will Entry Checks Cross the Line?, THE JAPAN TIMES (Nov. 8, 2007), http://search.japantimes.co.jp/print/nn20071108f1.html (describing statements of Barry Steinhardt, director of the ACLU’s Program on Technology and Liberty).
A. Utilizing Canadian Border Infrastructure for Exit-Data Collection

Executing a biometric exit-data collection procedure presents the most pressing need for US-VISIT’s success.168 While a complete infrastructure initiative at all border exits still remains unfeasible due to space constraints and considerable cost,169 US-VISIT officials could begin collecting data through immigration procedures already in place in Canada. There are already many examples of successful security cooperation between Canada and the United States.170 Thus, combining the infrastructure and staffing requirements at shared immigration checkpoints would allow for collection of biometric exit-data in the near future.

Joint Canada-U.S. immigration activities are already in use at Canadian airports and can provide a model for border crossings. To facilitate this relationship, the Canadian government passed the Preclearance Act in 1999171 and has authorized U.S. immigration officials to work at Canadian points of departure to the United States, inspecting foreign visitors who are bound for the United States.172 U.S. customs officials are currently posted in many of Canada’s airports and conduct pre-inspections for travelers flying to the United States.173 Further, “[i]f a person flies into the United States from Japan via Vancouver or Toronto, he or she will be greeted by [a] U.S. Customs and Border Protection inspector,” upon arrival in Canada.174

Through future cooperation with Canadian immigration officials, CBP could implement biometric data collection kiosks at these Cana-

169 See id.
170 The United States and Canada are both participants in the North Atlantic Treaty Organization, and collaborated on the North American Air Defense system (commonly referred to as “NORAD”). Canada has also been incorporated into the United States’ Strategic Defense Initiative, providing ballistic missile defense. The two countries have created an export perimeter control, requiring sensitive technologies to remain within their common borders. Several law enforcement joint task forces have also been established including Project North Star, Integrated Border Enforcement Teams, and Integrated National Security Enforcement Teams. See, e.g. John Noble, Fortress America or Fortress North America?, 11 LAW & BUS. REV. AM. 461, 467-71 (2005).
171 Preclearance Act, S.C. 1999, c. 20 (Can.).
173 Id.
174 Id.
adian points of entry for those travelers continuing on to the United States. This approach would have two advantages. First, it would speed immigration processing times at the United States point of entry because biometric data for travelers connecting through Canada would already have been taken. Second, it would prevent travelers that the United States considers “dangerous people” from boarding a commercial airliner bound for the United States, as well as prevent them from disembarking on U.S. soil.

Cooperation at border crossings, however, has seen political opposition stemming from the United States’ historical use of biometric identification technology. In 1999, U.S. immigration officials began reviewing commercial paperwork on the Canadian side of the Peace Bridge border crossing in Buffalo-Fort Erie for trucks bound for the United States. Customs officials intended to reduce congestion “caused by lack of advance document preparation.” In December 2004, the United States and Canada announced an expanded Shared Border Management (“SBM”) pilot project at the Peace Bridge. As part of the program, DHS had planned to conduct all primary and secondary border operations on the Canadian side of the border. Conducting inspections on the Canadian side made was advantageous because space to expand immigration and customs operations is greater on the Canadian side. A local neighborhood and a historic park constrain development on the U.S. side.

With the existing infrastructure present at border crossings, commentators have suggested that collecting biometric exit-data at Canadian points of entry represents the only feasible option. Because travelers exiting the United States must stop at the Canadian border to gain entry to Canada, collecting biometric exit-data in Canada would eliminate the need to build new infrastructure on the United States’

175 ABA Immigration and Nationality Comm., supra note 28, at 211.
176 Id.
178 Koslowski, supra note 172, at 540 (“Instead of building exit booths and staffing them with CBP officers to conduct primary exit inspections, Canadian Border Services Agency officers could simultaneously conduct their entry inspections together with U.S. exit inspections, so-called ‘reverse inspections.’”).
180 Id.
181 See, e.g., Koslowski, supra note 172, at 540 (noting that inspections on the Canadian side of the border “may be the best, if not the only, secure option short of building and staffing an exit infrastructure comparable to the existing entry infrastructure”).
side of the border and would ultimately reduce more traffic and congestion outbound from the United States. Canadian immigration officials at many land borders already collect I-94 forms from travelers departing from the United States and return them to U.S. immigration officials for processing; thus, the foundation for cooperation between the two countries’ immigration officials is already established.

In April 2007, however, both Canada and the United States withdrew from negotiations necessary to finalize the SBM program. The two countries could not agree on fundamental concerns regarding arrest authority and the right of U.S. officers to fingerprint travelers who come to the bridge, but decide not to cross. While U.S. Congressional leaders continue to call upon President Obama to renew negotiations with Canadian counterparts, commentators do not see a resolution to this impasse in the near future.

Specifically, Canadian negotiators argued that collecting biometric data in Canadian territory would violate Canada’s Charter of Rights and Freedoms (“Charter”). Section 15(1) of the Charter provides that: “[e]very individual is equal before and under the law and has the right to the equal protection and equal benefit of the law without discrimination and, in particular, without discrimination based on race, national or ethnic origin, color, religion, sex, age or mental or physical disability.” Commentators and Canadian negotiators analogized their fears that the SBM program would violate the Charter with those of human rights groups that criticized NSEERS. These

182 Id. at 538.
184 Id.
186 See, e.g., Ackleson, supra note 183, at 342-43 (noting that “[w]hile proponents of the initiative might hope for the plan to be revived in the new US presidential administration, this appears unlikely”); indeed, as the general manager of the Peace Bridge Authority remarked, “[i]t is highly improbable” that anyone in Washington will advocate for this program) (footnote omitted).
189 See, e.g., Frederic J. Moll, The Legal & Technological Advantage of a North American Perimeter in the War against Terrorism: How the Implementation of
groups argued that NSEERS’s implementation in Canadian airports under the Preclearance Act violated the Charter because it targeted travelers from primarily Muslim and Arabic countries. \footnote{Id.}

Canada intended the Preclearance Act to “avoid the extra-territorial application of US laws at these preclearance sites” and provided all travelers the full protections of Canadian law and the Charter. \footnote{Id. at 5.} If SBM is to maintain similar protections, the United States must guarantee that similar targeting does not occur in the future. This objective is met under the current US-VISIT program because its scope now includes all non-U.S. citizen travelers, regardless of country. \footnote{See BIOMETRICS AND YOU, supra note 2, at 1.} Thus, unlike under the NSEERS protocol, there is neither a need nor a possibility for U.S. or Canadian customs officials to profile travelers based upon their affiliation with any religion or ethnic group. With the ability to identify the biometric identity of all travelers, concerns over Charter violations could be mitigated. US-VISIT’s breadth and demonstrated effectiveness could lead to productive SBM negotiations in the future, providing a feasible avenue for the collection of biometric exit-data.

B. Extending the Reach of U.S. Border Protection by Creating a Common Biometric Data Collection Perimeter

Called the “longest, unprotected border,” the Canada-U.S. border stretches 5,525 miles and has 84 land border crossings. \footnote{ABA Immigration and Nationality Comm., supra note 28, at 202-203.} In 2000, figures indicated that approximately 130 million people cross the Canada-U.S. border each year and goods in excess of $1.5 billion cross the border each day. \footnote{Martin, supra note 18, at 333.} Canada exports about 82 percent of its goods to the United States, and the United States sends roughly 19 percent of its goods to Canada. \footnote{ABA Immigration and Nationality Comm., supra note 28, at 204.} Additionally, Canada is the biggest export market for thirty-nine U.S. states. \footnote{Id.}
Many Canadian officials and northern U.S. border states opposed the implementation of US-VISIT because they were concerned about the program’s potential impact on trade and tourism. Policies that increase border-crossing times would be severely detrimental to commercial interests of both countries. For instance, many corporations rely upon Just-In-Time (“JIT”) deliveries from across the border and delays could result in lost revenue and manufacturing shutdowns. Unsurprisingly, both nations recognize that overzealous border restrictions could devastate their respective economies, and that implementing US-VISIT exit-data collection procedures at the land border crossings would have at least a noticeable impact on the trans-border flow. GAO has also noted that US-VISIT exit-capabilities cannot be implemented at border crossings without “incuring a major impact” on those facilities.

National security concerns further complicate the problem because, as the Canadian Security Intelligence Service (“CSIS”) notes, “[w]ith the possible exception of the United States, there are more international terrorist organizations active in Canada than anywhere in the world.” According to CSIS, this is due to Canada’s proximity to the United States—the principal target of international terrorist organizations—and Canada’s accommodating immigration policies. Because of the prevalence of terrorist organizations in both the United States and Canada, an agreement over how to handle biometric data collection necessarily implicates important political policies.

While some commentators have underscored this tension between national security concerns and economic development, others have argued that U.S. national security depends upon maintaining open economic corridors; specifically, maintaining the economic relation-

---

197 Martin, supra note 18, at 333.
198 See ABA Immigration and Nationality Comm., supra note 28, at 204 (discussing the volume of commercial traffic between the United States and Canada, and noting it “precludes policies that would result in measurably longer crossing times”).
199 Id. at 209-10.
200 Id. at 208.
201 See Martin, supra note 18, at 333 (indicating that if each person crossing the border had to be checked on entry and exit it would obviously “curtail” some trade and tourism).
203 ABA Immigration and Nationality Comm., supra note 28, at 203 (citing CAN. SEC. INTELLIGENCE SERV., GOV’T OF CANADA, OPERATIONAL PROGRAMS: COUNTER-TERRORISM (revised Aug. 9, 2002)).
204 Id.
ship it has with Canada. Accordingly, as one commentator noted: “U.S. prosperity—and much of its power—relies on its ready access to North American and global networks of transport, energy, information, finance and labor. It is self-defeating for the United States to embrace security measures that end up isolating it from those networks.” Indeed, terrorists have repeatedly attacked United States economic targets in an attempt to undermine its security. Thus, maintaining a permeable border with Canada may have corresponding benefits for the security interests of the United States.

Taking into consideration the importance of border fluidity, the United States adopts the view that its borders must represent its last line of defense in that security “efforts must begin beyond U.S. territorial limits.” Thus, many national security policy proposals are based upon an attempt to “push U.S. borders out.” One policy proposal that has recently gained momentum involves the implementation of a “North American Perimeter” (“Perimeter”). Under a Perimeter regime, “internal border controls are lifted as a common external border is established.” Advocates for the policy argue that:

[harmonizing US and Canadian immigration and asylum policies would make it harder to organize attacks on the U.S. from Canada, and vice versa. If the two countries agreed on the criteria and used the same procedures for admitting foreign nationals, they could leave the Canada-U.S. border largely unguarded, benefiting trade and tourism.

The European Union has implemented a similar system, where 13 member nations participate in the collection of entry and exit-data, but

---

205 Id. at 206-07 (noting that a study conducted by the ABA’s Immigration and Nationality Committee, International Law Section concluded that “a less efficient border would be untenable from both an economic and a national security perspective”).


207 ABA Immigration and Nationality Comm., supra note 28, at 212.

208 Id. (linking economic prosperity to national security interests).

209 Id. at 216.

210 Koslowski, supra note 172, at 528.

211 Id. at 527.

212 Id.

213 Martin, supra note 18, at 339.
permit the free movement of people between the countries.214 Executed by the Schengen Agreement, members share access to a collective integrated border security database and present a common border check for foreign travelers.215 The fluidity of goods and people across European borders has been associated with notable economic growth in the region.216

Critics of the proposal argue that Perimeter would usurp Canada’s ability to set its own immigration policies, requiring it to harmonize its security and immigration policies with that of the United States.217 From a national security standpoint, critics point out that there are noticeable differences between Canadian and U.S. immigration policies that make coordination difficult. Indeed, several potential terrorists have been intercepted at the Canada-U.S. border,218 which has led to the perception that Canada’s immigration policies are more lenient than those of the United States.219

Adopting biometric data collection practices in Canada, however, would not necessitate a full implementation of a Perimeter; the parties could reach this result with a narrow agreement. A shared biometric data collection system could be set up independently and would not require the harmonization of visa and asylum policies, allaying Canadian concerns of losing control over its immigration policies. Additionally, a physical barrier between the United States and Canada would still exist for those concerned about opening the border to completely unrestricted travel.

Under this policy initiative, the need to confirm a traveler’s identity at the Canada-U.S. border would be eliminated. Travelers who enter the United States over the Canada-U.S. border would have already had their identity confirmed upon entering Canada. Determining the true identity of travelling Canadians would also not be necessary because under the current US-VISIT regime, Canadians are exempt from biometric data collection protocols.220 Thus, biometric data collection

214 Id. ("[The European Union’s Schengen Agreement] currently permits free movement among 13 member nations, with entry and exit controls for all done by participating countries, so that a flight from Madrid to Paris is treated as an internal flight.").
215 Id.
216 Id.; see also Miller, supra note 55, at 187-88 (discussing the relationship between integration and economic growth in the European Union).
217 Koslowski, supra note 172, at 541.
218 See, e.g., ABA Immigration and Nationality Comm., supra note 28, at 202-03 (describing terrorist plots foiled at the border U.S.-Canadian border).
219 Martin, supra note 18, at 339 (highlighting a case in which an individual with a criminal history was able to use a forged document to obtain a Canadian driver’s license and passport under a false name).
220 See U.S.-CANADA BORDER, supra note 62.
at Canada-U.S. border checkpoints would not be necessary, facilitating the flow of legitimate travel. Such a program would allow the United States to uphold the objectives set forth by US-VISIT, but continue to provide a relatively open border with Canada. Similar to the proposed SBM approach, US-VISIT’s scope includes all foreign travelers, not just those from targeted countries. Thus, Canadian concerns over potential Charter violations through profiling could be eliminated.

C. Implementing Alternative Exit-Data Collection Technologies

1. RFID Tagging in I-94 Forms

While building exit-data collection facilities identical to those found upon points of entry would be cost-prohibitive, several emerging identification technologies exist that could be used to similar effect. For example, Radio Frequency Identification (“RFID”) technology has been tested at several land border crossings since 2006.221 RFID technology comprises a microchip with an antenna that transmits a unique signal wirelessly to a receiver that reads the signal.222 Beyond the border security context, other industries have utilized RFID technology as part of their business strategy. For instance, credit card companies have begun to embed RFID chips in their cards and have marketed this “PayPass” technology as an ability for consumers to swipe cards wirelessly.223 Retailers are also using RFID chips to track goods for supply-chain management purposes.224

Chips embedded in I-94 forms can transmit data to radio receivers located at border exit points.225 RFID chips can transmit to receivers 20 feet away,226 allowing officials to capture the information instantaneously when travelers cross the border without requiring automobile or pedestrian traffic to stop at the border. This technology would allow U.S. border officials to track electronically those travelers carry-

223 Id.
224 Id.
225 U.S. Gov’t Accountability Office, GAO-07-248, Border Security: US-VISIT Faces Strategic, Operational, and Technological Challenges at Land Ports of Entry 7 (2006) (“RFID technology can be used to electronically identify and gather information contained on a tag...which an electronic reader at the [port of entry] is intended to detect.”).
226 Garskof, supra note 213, at 48.
ing their I-94 Forms when leaving the United States.\textsuperscript{227} Such an implementation would be similar to the electronic highway toll EZ-Pass system, where RFID transmitters track individual vehicles as they pass through tolls without stopping.\textsuperscript{228}

However, performance and reliability problems suggest that this approach is not a feasible long-term solution. Furthermore, the data embedded in the forms is not biometric and does not fulfill DHS’s mandate to implement a biometric entry-exit tracking system.\textsuperscript{229} Indeed, the tracking system would not be able to track the exit of those individuals who do not carry their I-94 forms when leaving the country or those individuals who carry another’s I-94 form for the purpose of deceiving the exit-data collection system. Thus, it is only a temporary solution.\textsuperscript{230}

2. Iris Recognition Technology

While not currently implemented, DHS has expressed interest in expanding the biometric data collection procedures to include iris recognition technology.\textsuperscript{231} The technology scans the distinct characteristics of an individual’s iris—the colored ring surrounding the pupil.\textsuperscript{232} Other countries have already implemented iris recognition at immigration checkpoints. For instance, the United Kingdom, Canada, and the Netherlands each allow frequent travelers to enroll in programs that register the individual’s iris pattern in order to expedite the immigration process.\textsuperscript{233} Singapore uses iris recognition to identify and

\textsuperscript{228} FRANK THORNTON ET AL., RFID SECURITY 27-28 (Syngress Publishing 2006).
\textsuperscript{229} U.S. GOV’T ACCOUNTABILITY OFFICE, GAO-07-248, BORDER SECURITY: US-VISIT FACES STRATEGIC, OPERATIONAL, AND TECHNOLOGICAL CHALLENGES AT LAND PORTS OF ENTRY 7 (2006) (“[T]he RFID solution does not meet the statutory requirement for a biometric exit capability because the technology as tested cannot meet a key goal of US-VISIT—ensuring that visitors who enter the country are the same ones who leave.”).
\textsuperscript{230} Id.; see also Kenneth A. Bamberger & Deirdre K. Mulligan, PRIVACY DECISION-MAKING IN ADMINISTRATIVE AGENCIES, 75 U. CHI. L. REV. 75, 94 (2008) (exploring DHS’s investigation into the possibility of using RFID chip technology on Form I-94s to track individuals electronically).
\textsuperscript{231} ENHANCING SECURITY, supra note 4, at 3 (US-VISIT continues to “explore[e] multimodal biometrics like iris and facial recognition....”).
\textsuperscript{232} U.S. GOV’T ACCOUNTABILITY OFFICE, GAO-03-174, TECHNOLOGY ASSESSMENT USING BIOMETRICS FOR BORDER SECURITY 193 (2002). In fact, the probability of two individual’s possessing the same iris pattern is estimated to be one in seven billion. Id.
\textsuperscript{233} Id. at 199-201.
admit approximately 50,000 workers that travel from Malaysia each 
day.234 Since 2001, the United Arab Emirates ("UAE") has imple-
mented a mandatory iris scan for every foreigner entering the coun-
try.235

Recent developments in iris scanning technology suggest that it 
would be an effective alternative to fingerprint scans. Previous gen-
erations of iris recognition technology required individuals to stand 
three to ten inches from the scanner.236 However, newer-generation 
scanners can recognize the iris of an individual standing fifteen meters 
away.237 Furthermore, the time required to match an iris pattern within 
a database is minimal using current technology. UAE officials report 
that iris recognition searches typically take about one second.238

With these recent advances in iris scanning technology, the Uni-
ted States could require individuals leaving the country to look at a 
scanner by the side of the road. Such an installation would not require 
the heavy investment in infrastructure and personnel necessary to 
support an exit-data collection procedure mimicking that specified for 
entry. Furthermore, travelers would not need to stop and be processed 
individually by immigration officials.

Even if US-VISIT officials utilize iris scanning technology at 
borders, they should not discontinue the use of all fingerprinting 
throughout the program. The iris scan could take place simultaneously 
with the fingerprint scan or during the facial photograph when the 
foreigner is entering the country. Therefore, US-VISIT would still be 
able to harness the power of the FBI’s fingerprint database, but be 
able to use iris data to record the exit of those individuals later. Using 
multiple forms of biometric identification may be a feasible way to 
track both the entry and exit of foreign visitors.

CONCLUSION

While DHS asserts that the US-VISIT program has experienced 
reasonable success in meeting its objectives, there still exist areas for 
improvement in its biometric collection procedures. The difficulties in 
collecting biometric exit-data for travelers leaving the United States

234 Id. at 201.
235 BIOMETRICS: THEORY, METHODS, AND APPLICATIONS 316 (Nikolaos v. 
Boulgouris et al. eds., 2010).
236 U.S. GOV’T ACCOUNTABILITY OFFICE, GAO-02-174, TECHNOLOGY 
ASSESSMENT USING BIOMETRICS FOR BORDER SECURITY 194 (2002).
237 Karl Ricanek Jr. et al., Unconstrained Biometric Identification: Emerging 
Technologies, 43 COMPUTER 56, 60 (2010).
238 BIOMETRICS: THEORY, METHODS, AND APPLICATIONS, supra note 235, at 
318.
remains one of the primary gaps DHS must resolve in order to comply with its mandate for a biometric tracking system. Cooperation with Canadian border officials under the proposed SBM scheme could alleviate the infrastructure requirements at border crossings that prevent DHS from implementing exit-data collection. In future SBM negotiations, US-VISIT’s expanded scope can resolve Canadian fears of Charter violations that allegedly occurred under the NSEERS program. Alternatively, the two countries could implement a policy initiative that would resemble a common biometric identification perimeter. Such a program would promote reduced transaction costs for businesses at border crossings, while maintaining the security objectives set forth by US-VISIT. If Canada and the United States are unwilling to collaborate, US-VISIT could deploy alternative biometric collection technologies such as iris recognition, which may make the collection of exit-data information more feasible.

Mark Skerry†

† J.D. Candidate 2011, Case Western Reserve University School of Law; B.S. 2007, Cornell University.