Order Code RS21916
Updated February 7, 2005

Biometric Identifiers and Border Security: 9/11 Commission Recommendations and Related Issues

Daniel Morgan and William Krouse
Resources, Science, and Industry Division and
Domestic Social Policy Division

Summary

In its final report, the 9/11 Commission concluded that funding and completing a "biometric entry-exit screening system" for travelers to and from the United States is essential to our national security. The commission noted that the United States has built the first phase of a biometric screening system known as US-VISIT, and recommended that the "patchwork" of other border screening systems be consolidated with US-VISIT to serve as the basis for a single system to streamline border inspections. This report provides an overview of biometric technologies and the major U.S. biometric border screening systems, including US-VISIT, and discusses issues such as cost, performance, and user acceptance. Based in part upon the commission's recommendations, Congress included biometric provisions related to entry/exit control in the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458). This topic will probably continue to be of interest to the 109th Congress. This report will be updated as needed.

Introduction

The National Commission on Terrorist Attacks Upon the United States, commonly known as the 9/11 Commission, found that "constraining terrorist travel should become a vital part of counterterrorism strategy." Noting that "false identities are used by terrorists to avoid being detected on a watchlist" and that "biometric identifiers make such evasions far more difficult," the commission recommended that

> The Department of Homeland Security, properly supported by the Congress, should complete, as quickly as possible, a biometric entry-exit screening system, including a single system for speeding qualified travelers.

The commission identified the United States Visitor and Immigrant Status Indicator Technology program (US-VISIT) as the first phase of such a program, and recommended that this system be fully integrated with other border screening systems. It further

recommended that biometric passports (or other secure identity verification) should be required of all travelers entering the United States, including U.S. citizens.[1]

Overview of Biometric Technologies and Applications

Biometrics are physical or behavioral characteristics of a person that can be measured and used for identification. Fingerprint patterns are a familiar example. Of the biometric technologies so far deployed or tested by border security agencies, fingerprints and face recognition are the most commonly used, and iris scans are widely viewed as promising for future applications. Images and measurements of biometrics are typically digitized and reduced to a numerical identifier that is unique to a particular person. Biometric identifiers can then be used for two distinct purposes, identity verification and identity discovery. In other words, they can answer two questions: Is this person really who he says he is? and Who is this person?[2]

Identity Verification. In an identity verification application, a person enrolls in the system, and his identifying data are measured and recorded in a database or on a document. To confirm the person's identity later, his identifying data are measured again and compared with the original. This is known as one-to-one matching. An accurate system will confirm a true claim of identity and reject a false claim with high probability. Border security applications include verifying the identity documents of border crossers, including pre-enrolled trusted travelers.

Identity Discovery. Identity discovery is more challenging than identity verification. If a person makes no claim of identity, or if his claimed identity may be false, then his identifying data must be compared with the stored data of all possible matches. This is known as one-to-many matching. Because many comparisons are made in identity discovery applications, the likelihood of a coincidental match, or even multiple matches, is increased. Moreover, identity discovery may be impossible if biometric data are simply not available for some target individuals. For example, a fingerprint check cannot identify a traveler as a suspected terrorist if the terrorist's fingerprints are not known.

Leading Biometric Technologies. The most widely used biometric technology is *fingerprint recognition*, based on the pattern of ridges on the fingertips. Fingerprint patterns have been used in law enforcement since the 1800s, and automated systems have been commercially available since the 1970s. *Hand geometry*, based on the dimensions of the fingers, joints, and knuckles, has been used for about 30 years to control access to secure facilities such as nuclear power plants. *Facial recognition* analyzes features such as the eye sockets, cheekbones, and sides of the mouth. It has the advantage that cameras can capture facial images remotely. *Iris scanning* technology analyzes the visible patterns in the colored iris of the eye. These patterns reportedly remain stable throughout one's lifetime, and can be scanned without physical contact. All four of these technologies have been used in one or more border control applications, including programs in the United

---

[1] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington, 2004), pp. 385-389.

[2] A third purpose for biometric systems, identity exclusion, is effectively the opposite of identity verification. For example, in a law enforcement setting, fingerprints may be used to rule out a particular suspect as the perpetrator of a crime.

States, Australia, Britain, Canada, Hong Kong, Israel, the Netherlands, Saudi Arabia, and Singapore. Other biometric technologies include retinal scanning, signature recognition, voice recognition, and numerous emerging techniques of varying technological maturity.[3]

Interpreting Accuracy Claims. Claims for the accuracy of biometric technologies often require careful interpretation for several reasons. First, matching can fail in two ways: a false positive, which is an incorrect match between the identifiers of two different people, or a false negative, which is an unsuccessful match between two measurements of the same person. Second, in any system, the criteria used for matching can be adjusted from more stringent to less stringent. In a given system, requiring greater similarity before declaring a match will generally reduce false positives at the cost of increasing false negatives, and vice versa. The appropriate tradeoff may vary from application to application, even for a single technology. Third, in one-to-many matching, the size of the stored database strongly affects the likelihood of a coincidental match. Despite these factors, equipment vendors often quote just one accuracy figure known as the equal-error rate (EER): the accuracy of one-to-one matching when the matching criteria are chosen to make the false positive rate equal to the false negative rate.

Current U.S. Biometric Systems and Border Security

In the past decade, digitized biometrics (principally fingerprints) have been developed to identify individuals with greater certainty. While the commission identified US-VISIT as the first phase of a biometric entry/exit screening system, it also recommended that this system be more fully integrated with other border screening systems.[4] Major U.S. law enforcement and border security biometric systems are described below, but this treatment is not exhaustive and there are many other systems that might warrant integration.

Integrated Automated Fingerprint Identification System (IAFIS). While most biometric technologies have been developed only in the past 10-15 years, fingerprints have been used by law enforcement to verify identity for the past century. For these purposes, the Department of Justice's (DOJ's) Federal Bureau of Investigation (FBI) maintains the Integrated Automated Fingerprint Identification System (IAFIS), an automated 10-fingerprint matching system that captures rolled prints. All 50 states are connected to IAFIS for searches, and 47 participate by submitting new data. With over 47 million sets of fingerprints, IAFIS is the largest biometric database in the world.[5]

Automated Biometric Fingerprint Identification System (IDENT). In 1995, the former Immigration and Naturalization Service (INS) piloted a two flat fingerprint system known as IDENT. This system includes the prints of 4.5 million noncitizens.

---

[3] For a more detailed survey of biometric technologies and their applications, see U.S. General Accounting Office, *Technology Assessment: Using Biometrics for Border Security*, GAO-03-174, Nov. 2002.

[4] For further information on other terrorist screening systems and watch lists, see CRS Report RL32366, *Terrorist Identification, Screening, and Tracking Under Homeland Security Presidential Directive 6*, by William J. Krouse.

[5] GAO, *Technology Assessment*, p. 149.

Some Members of Congress, serving on the Appropriations Committees, voiced concern that two incompatible fingerprint identification systems were being developed. This issue was elevated following revelations that immigration agents had released aliens with serious criminal records, who subsequently reentered the United States and committed murder. The Attorney General initiated an IDENT/IAFIS integration project, but the transfer of the INS from DOJ to the Department of Homeland Security (DHS) hampered the progress of this project. Despite a two year delay, a partially integrated IDENT/IAFIS system was available in December 2003. Full deployment, however, may extend past FY2008. About 4,500 FBI fingerprint files of known or suspected terrorists have been entered into IDENT.[6]

National Security Entry-Exit Registration System (NSEERS). Following the 9/11 attacks, the IDENT system was linked into NSEERS, a program under which the nationals of certain countries — and other foreign nationals who meet undisclosed security or law enforcement criteria — who travel to the United States on nonimmigrant (temporary) visas are required to register with DHS upon arrival in the United States and to deregister upon departure. Among other requirements, travelers must be photographed and fingerprinted.[7]

US-VISIT. As required by Border Security Act (P.L. 107-173), the US-VISIT program was developed by DHS as an automated biometric entry/exit control system to track the arrival and departure of foreign travelers. Under this program, most foreign visitors traveling to the United States on a visa have their index fingers scanned (with IDENT) and a digital photo taken to verify their identity at the port of entry.[8] Under US-VISIT, biometric queries through IDENT/IAFIS are made of several databases, including FBI "hot files" on known and suspected terrorists, wanted persons, and sexual offenders. By September 30, 2004, these procedures will be expanded to include foreign travelers from the 27 countries that participate in the Visa Waiver Program — a program that was established in 1986 and made permanent in 2000. US-VISIT is operational at 115 airports and 14 seaports, and is scheduled to be deployed at the 50 busiest land ports by December 31, 2004, and all ports of entry by December 31, 2005. Congress included provisions requiring the expedited implementation of this program in P.L. 108-458.

Consular Consolidated Database (CCD). The Department of State (DOS) has established the capacity at consular posts abroad to capture electronic records of immigrant and nonimmigrant visas, including digitized visa photos and fingerprints, which are transmitted and replicated in State's CCD.[9] In FY2001, the DOS and INS conducted a pilot visa data-sharing program at the Newark International Airport. Later, for purposes of identity verification, visa records, including digitized photos and

---

[6] U.S. Department of Justice, Office of the Inspector General, Report No. 1-2003-005, *Status of IDENT/IAFIS Integration*, (Washington, Feb. 2004), pp. 11 and 18.

[7] For further information, see CRS Report RL31570, *Immigration: Alien Registration*, by Andorra Bruno.

[8] For further information, see CRS Report RL32234, *U.S. Visitor and Immigrant Status Indicator Technology Program (US-VISIT)*, by Lisa Seghetti and Stephen Viña.

[9] For further information, see CRS Report RL31512, *Visa Issuances: Policy, Issues, and Legislation*, Ruth Ellen Wasem.

fingerprints, were transmitted to the Bureau of Customs and Border Protection's Interagency Border Inspection System. This capability reportedly has been deployed at all air ports of entry, but the photos do not currently include a biometric component. To this end, however, DOS has also begun phasing in the use of facial recognition technologies with visa and passport photos, but these technologies are less mature than those using fingerprints. The member states of the International Civil Aviation Organization (ICAO), to which the United States is a party, have approved interoperable biometric standards, and the baseline biometric will be facial recognition. Member states will also have the option of adding fingerprints or iris scans.[10]

Visa Waiver Program and Biometric Passports. The Border Security Act requires that in order to remain eligible for the Visa Waiver Program, participating countries must issue their nationals machine-readable passports that include biometric identifiers. In August 2004, the act's original deadline for biometric passport issuance, October 26, 2004, was extended by one year (P.L. 108-299).[11] As most border-related practices hinge on the principle of reciprocity, the DOS has developed a comparable passport for U.S. citizens traveling abroad. Scheduled for issuance in Spring 2005, it will include an embedded microchip that stores facial geometry characteristics.[12] The 108th Congress considered biometric passport provisions in S. 2845 and H.R. 10, but these provisions were not included in P.L. 108-458.

Issues

Cost. The cost of biometric systems like those recommended by the 9/11 Commission would be substantial and recurring. Funding for US-VISIT in FY2004 was $328 million. In 2002, the GAO estimated that incorporating biometrics into visas would cost between $700 million and $1.5 billion per year, depending on the number of applicants and the type of biometric technology used, and incorporating biometrics into U.S. passports would cost between $1.6 billion and $2.4 billion per year. The initial costs of planning and fielding the systems are not included in these GAO estimates.[13]

Performance. As noted above, performance claims for biometric technologies should be interpreted carefully. Performance depends on the details of how a technology is to be used, as well as on factors like lighting conditions (for facial recognition) and dirt and wear (for fingerprints). Some biometrics may vary as a person ages. Some can probably be masked intentionally by altering one's appearance. Some cannot be used by individuals whose relevant body parts are absent or damaged. For identity discovery applications, such as matching against a watchlist, speed and performance depend

---

[10] Statement of Frank E. Moss, Deputy Assistant Secretary for Passport Services, Bureau of Consular Affairs, Department of State, on June 23, 2004, before the House Committee on International Affairs. See [http://wwwc.house.gov/international_relations/108/mos062304.htm]. See also the ICAO biometrics website, [http://www.icao.int/mrtd/biometrics/intro.cfm].

[11] For further information, see CRS Report RL32221, *Visa Waiver Program*, by Alison Siskin.

[12] See, for example, Jonathan Krim, "Passport ID Technology Has High Error Rate," *Washington Post*, Aug. 6, 2004, p. A01, and Junko Yoshida, "U.S. E-Passport Plan Raises Tech, Diplomatic Hackles," *EE Times*, July 19, 2004.

[13] GAO, *Technology Assessment*, pp. 108-114.

strongly on the size of the database, which determines the number of matches that must be evaluated. The time required for enrollment and matching varies between technologies. Comparing alternative approaches requires a uniform testing methodology that reflects all these challenges.

Security. Most biometric technologies have demonstrated vulnerabilities to intentional deception. For example, facial recognition and iris scanning can sometimes be defeated by presenting a picture of someone else's face or iris. In border security applications, however, the presence of a human operator makes such techniques less likely. Information security is a more likely concern, including unauthorized changes to or disclosure of biometric data stored in a central database or on an identity document.

User Acceptance. Privacy concerns include the protection of personal data against misuse, perhaps including identity theft; the possibility of "function creep," or the eventual use of biometric data for purposes other than border security; the loss of personal anonymity; and the possibility that some biometric data may reveal personal medical information. Some users may have concerns about specific technologies: the hygiene of fingerprint scanners or the association of fingerprints with criminals, for example.

Standards. Effective use of biometrics requires standards for the type of data collected, the physical format in which data are stored (if they are stored on a document such as a passport), and the software format for data collection and interchange. The National Institute of Standards and Technology (NIST) is the lead federal agency in this area.[14] The private, nonprofit American National Standards Institute (ANSI) has also issued a number of U.S. standards for biometrics, as have several other private-sector organizations. For border security applications, international standards are essential. The ICAO, an intergovernmental body that operates under the United Nations, has recommended standards for biometrics in travel documents such as visas and passports.[15] ICAO's recommendations include the worldwide use of facial recognition to ensure interoperability and the storage of identifiers in contactless integrated-circuit chips embedded in documents. Additional standards work is conducted by the nongovernmental International Organization for Standardization (ISO), of which ANSI is the U.S. member.

Related Applications of Biometrics

Since the 9/11 terrorist attacks, biometric technologies have been proposed for a number of other homeland security applications. Many of these involve controlling access to secure areas. For example, several airports have tested or deployed biometric technologies for access control. In August 2004, the Transportation Security Administration began the prototype phase of developing a uniform Transportation Worker Identification Card, which will include a biometric. Facial recognition has been widely proposed, and less widely used, for surveillance in public places such as airports and sports stadiums, although its effectiveness for this purpose has been questioned. These and other applications are beyond the scope of this report, but experience with them may be instructive for efforts to incorporate similar technologies into border security.

---

[14] For further details, see the NIST Information Technology Laboratory website on standards for biometrics: [http://www.itl.nist.gov/div893/biometrics/].

[15] See [http://www.icao.int/mrtd/biometrics/intro.cfm].