Considerations on the Emerging Implementation of Biometric Technology

by
ROBIN FELDMAN*

* Assistant Professor, University of California, Hastings College of the Law. I am greatly indebted to David Faigman, Reuel Schiller, James Wayman, and John Woodward for their comments on prior drafts. I am also grateful to Amy Hsiao for her research assistance. A draft of this paper was presented at the 2003 COMM/ENT Symposium at UC Hastings.

I. Introduction

Biometrics is the science of identifying people based on their physiological and behavioral characteristics.[1] Modern technology offers the tantalizing prospect of rapid and accurate identification using features such as characteristics of the hand, patterns in the eye, and facial geometry. Although biometric science could revolutionize the process of identification, it also raises concerns that should be considered as we enter into more widespread use of the technologies.

Concerns about biometrics are particularly important in light of the federal government's project to implement biometric technologies at all points of entry by the end of 2004. Following a Congressional mandate, all visas for entry into the United States must include biometric data by October 26, 2004.[2]

Technological and diplomatic challenges will prevent full implementation by the October deadline.[3] Nevertheless, the federal initiative is proceeding at a rapid pace. The Department of Homeland Security expects to have fingerprint and face scanners in place at 115 airports by January of 2004.[4] These systems will collect biometric information from all visitors coming through immigration, data which will be checked against a terrorist watch list. The government expects to have fingerprint and face scanners in place in all airports and sea ports by the end of 2004, with land crossings included within the next few years.[5]

Much of the discussion surrounding implementation of biometric technology involves developing rules to ensure reliability of the systems and create appropriate restrictions on the use of the data.[6] This article argues, however, that regardless of how much we invest in establishing standards for reliability of the technology and protections of the data from fraud or improper use, no system will be foolproof. Biometric determinations will be subject to mistakes, fraud, and

1. *See* H.R. Subcomm. on Domestic and Intl Monetary Policy of Comm. on Banking and Financial Services, *Hearings on Biometrics and the Future of Money*, 105th Cong. 6 (May 20, 1998) [hereinafter *Biometrics and the Future of Money*] (statement of Jeffery S. Dunn, Chairman of Biometrics Consortium).

2. *See* Brian Bergstein, *U.S. Now Demanding Biometric Technology*, AP – Technology (Aug. 25, 2003) (available in 2003 WL 62376790).

3. *See id.*

4. Deborah Charles, *U.S. Unveils High-Tech Foreign Registration Program*, Reuters <http://www.reuters.com/newsArticle.jhtml?type=topNews&storyID=3707411> (Oct. 28, 2003).

5. *See id.*; Bergstein, *supra* n. 2.

6. *See, e.g.,* sources cited *infra* n. 93.

abuse through human and technological error, both intentional and inadvertent. As a result, we should take this opportunity to develop methods for individuals to review and challenge biometric determinations. In particular, the article suggests a doctrinal framework for challenges to biometric determinations made by administrative agencies.

At the most basic level, biometric data is simply data. Its collection, therefore, raises the same concerns we have when the government or private groups collect any data. Given that other symposium presenters will discuss data collection and data mining in general, I will focus primarily on 1) describing issues that might cause greater concern in the case of collection of biometric data than in the case of collection of other personal identification data, such as addresses or social security numbers, and 2) proposing a framework particularly appropriate for biometrics.

II. Biometric Technology and Uses

A. Overview

Biometric technology uses automated methods for recognizing a person based on physiological or behavioral characteristics.[7] Fingerprints are the most commonly used and widely accepted form of biometric data. Other biometric technologies currently in use are based on hand and finger geometry, eye scans, facial imaging, and speaker recognition. Techniques under investigation include identification by vein patterns, gait, sweat pores, body odor, and brain waves.[8]

Biometrics can be used in two ways: 1) to verify that people are who they say they are and 2) to identify unknown people.[9] For example, suppose someone arrives at an access point claiming to be John Doe. An automated system can analyze the biometrics of the person trying to enter and compare it to biometric information about

7. *See Biometrics and the Future of Money*, *supra* n. 1, at 4.

8. *See* John D. Woodward, Jr., Nicholas M. Orlans, & Peter T. Higgens, *Esoteric Biometrics,* in *Biometrics* 115, 115-136 (Jane K. Brownlow, ed., McGraw-Hill 2003); Anil K. Jain, Ruud Bolle, & Sharath Pankanti, *Introduction to Biometrics*, in *Biometrics: Personal Identification in Networked Society* 1, 10-11, 13 (Anil K. Jain, et al., eds., Kluwer Academic Publishers 1999).

9. *See* Samir Nanavati, Michael Thieme, & Raj Nanavati, *Biometrics: Identity Verification in a Networked World* 12-14 (2002); Richard E. Smith, *How Authentication Technologies Work*, in *Biometrics* 3, 7 (Jane K. Brownlow, ed., 2003).

John Doe already in the database. This process is known as verification, or one-to-one matching.[10]

In contrast, identification, or "one-to-many" matching, requires the system to read a person's biometrics and scan a large database to find a match.[11] An FBI search for a fingerprint match found at a crime scene would be an example of identification. Technologically, it is much easier to verify who you claim to be with reasonable accuracy than to identify an unknown person. In particular, only fingerprints and retinal scanning have been shown in independent tests to scan databases containing more than 1,000 entries, although other technologies could develop to that point.[12]

Most biometric systems operate by translating information about a human feature into a mathematical construction. The mathematical construction has no physiological meaning. Rather, the information developed by the computer is only indirectly related to physiological features.

Consider a hypothetical attempt to develop a formula for comparing noses. A *direct* comparison would take physiological measurements of a particular person's nose, such as the length of the bridge, the size of the nostril opening, and the width of the tip. The computer would store the information, take measurements again when the subject returns, and compare the two. The identity would be verified only if enough of the information matched. One could also imagine a system taking an initial image, like a photograph, of the nose. When the subject appears for verification, the system would superimpose the second image over the first, detecting variations in the physical measurements.

Current automated biometric systems do not work in this way at all.[13] Rather, the systems are based on developing mathematical formulas to detect statistically significant correlations among the

10. Smith, *supra* n. 6, at 8. One-to-one matching also may be written as (1:1).

11. *See id.* at 7-8. One-to-many matching also may be written as (1:N).

12. *See* H.R. Subcomm. on Domestic and Intl Monetary Policy of Comm. on Banking and Financial Services, *Hearings on Biometric Identification and the Financial Services Industry,* 105th Cong. [3] (May 20, 1998) (statement of James L. Wayman, Director, U.S. national Biometric Test Center). Independent testing, at least up until 1998, has shown that facial geometry, speaker recognition and hand geometry are not capable of identifying an individual from a database of greater than 1,000.

13. The problem with a hypothetical direct comparison system can be described in terms of not enough variation and too much variation. Human noses may not vary enough to allow identification or verification through simple, direct measurements. In addition, the information must be grouped in some way that allows efficient processing. Too much undifferentiated information is unmanageable.

elements of abstracted patterns of human characteristics.[14] Consider again the hypothetical project to develop a nose biometric. System developers could begin by extracting a mathematical representation of the noses of a sample of the population. The representation would not be an actual image of the people in the database. Rather the nose scanning device could scan to create a one-dimensional pattern representation of the elements of the noses.[15]

Once the pattern information has been extracted, developers would run computer analyses of the data set made up of the patterns of all of the people in the population sample, trying to find relationships in the patterns that would consistently allow differentiation of individual noses from the group. That relationship could be expressed, for example, as a formula which takes the derivative of the relationship between the mathematical abstraction of one part of the pattern and another part of the pattern. In other words, one might find that washing the pattern data through the formula consistently yields a result that allows us to distinguish individual noses from the group. The formula, or algorithm, would provide the basis for determining whether the nose of the person requesting access has a high correlation with the nose of the person enrolled in the system. In sum, biometric systems generally are based on algorithms that analyze abstracted pattern representations of human characteristics.

B. Individual Technology and Uses

Fingerprinting, based on comparing the graphical, flow-like ridges of the fingers, is the oldest and most familiar biometric.[16] Fingerprinting techniques appeared in scientific literature as early as the seventeenth century, and the use of a fingerprint to identify a criminal suspect can be traced to the 1870s.[17]

14. *See* Jain et al., *Introduction to Biometrics*, *supra* n. 8, at 1, 21. For a classic, technical explanation of pattern recognition, see Keinosuke Fukunaga, *Introduction to Statistical Pattern Recognition* (2d ed., Academic Press, New York 1990).

15. For example, retinal scanning devices do not take images of the retina, but rather scan the retina in a circle to create a one-dimensional pattern. *See* Robert "Buzz" Hill, *Retina Identification*, in *Biometrics: Personal Identification in Networked Society* 123, 126-27 (Anil K. Jain, et al., eds. 1999).

16. *See* Peter T. Higgins, *Fingerprint and Hand Geometry,* in *Biometrics* 45, 45 (Jane K. Brownlow, ed., 2003); Anil K. Jain, Lin Hong, Sharath Pankanti, Ruud Bolle, *An Identity-Authentication System Using Fingerprints,* 85 Proceedings of the IEEE 1365, 1367 (Sep. 1997).

17. *See* Jain, et al., *supra* n. 16, at 1367-68; Higgins, *supra* n. 16, at 45-47. While serving as a missionary doctor in Japan in the 1870s, Dr. Henry Faulds became interested in fingerprint impressions embedded in ancient pottery. His interest led him to take

The FBI currently has tens of millions of fingerprints in its database.[18] The system can provide a match for fingerprints taken from a suspect at the time of an arrest in less than two hours.[19] The use of fingerprinting technology, however, is not limited to criminal investigation. The majority of fingerprint searches conducted by the FBI are for employee background checks.[20] In addition, fingerprint identification is used by a variety of private commercial enterprises and regulatory agencies including commercial check cashing entities, state motor vehicle departments and notaries.[21]

Facial imaging technology describes a group of different approaches designed to reduce facial qualities to mathematical abstractions that can be captured and evaluated electronically. The technologies vary in terms of the types of information analyzed and the method of analysis. The term "Eigenfaces," for example, refers to a broad class of algorithms that represent and compare individual faces by reference to abstracted images of archetypal faces.[22] The process includes subtracting the abstracted representations of an average face from the abstracted representations of the particular face being enrolled to create mathematical variants.[23]

All of the facial imaging technologies work best with a well-lit frontal image, such as a mug shot, rather than images extracted from faces in a moving crowd.[24] Government testing suggests a 75-80 percent accuracy rate in stationary, frontal-image tests designed to simulate real-world conditions, with a higher accuracy rate under ideal conditions.[25] Critics charge, however, that even the 75-80percent

samples of fingerprints from his students. When a beaker of alcohol was stolen from his lab, Faulds used the fingerprint samples to identify one of his students as the culprit. *See id.*

18. *Id.* at 55.

19. *Id.*

20. Vance C. Bjorn, *An Introduction to Privacy and Security Considerations of Biometrics Technology,* 701 PLI/Pat. 105, 107 (2002).

21. *See* Alexander T. Nguyen, *Here's Looking at You, Kid: Has Face-Recognition Technology Completely Outflanked the Fourth Amendment?*, 7 Va. J.L. & Tech 2, 3 (2002) (noting fingerprint requirements for receiving welfare, driver's licenses, and cashing checks); Juan Espinosa, *Businesses May Require Fingerprint to Cash Checks*, Knight-Ridder Tribune Bus. News (Dec. 7, 2001).

22. *See* Nicolas Orlans, *Facial and Voice Recognition,* in *Biometrics* 71, 75 (Jane K. Brownlow, ed., 2003).

23. *See* David Shenk, *Watching You: The World of High-Tech Surveillance*, 204 no. 5 Natl. Geographic 3, 18 (Nov. 2003).

24. *See* Nanavati et al., *supra* n. 9, at 70; Orlans, *supra* n. 22, at 73.

25. *See* Nanavati et al., *supra* n. 9, at 76.

rate is high given that real-world conditions are more challenging than any form of simulation.[26]

Despite the added difficulties of scanning faces moving in a crowd, facial imaging technology was used during the Super Bowl in January of 2001. Cameras equipped with facial imaging software scanned individual faces in the stadium, attempting to match the data against known criminals.[27] No arrests were reported.[28]

Similarly, a crowd scanning project in Tampa, Florida, produced disappointing results. For two years, the Tampa police department used cameras distributed in a section of the town and equipped with facial imaging software to capture images of passing faces. The images were compared to a database of 30,000 fugitives, runaways, and sexual predators.[29] The project was terminated in August of 2003 after failing to yield a single positive identification.[30]

The Department of Motor Vehicles in West Virginia also has used facial imaging technology to try to prevent driver's license fraud.[31] Photos of new applicants are compared to a database of photos of existing license holders, and the applicant is challenged when there is a discrepancy.[32] Six thousand licenses have been denied in the first five years of operation.[33]

Although the West Virginia DMV considers the number of denials a mark of the amount of fraud avoided,[34] this may be an overbroad interpretation of the data. The raw numbers do not establish how much fraud was deterred as opposed to how many errors occurred.

---

26. *See id.*

27. *See* Nguyen, *supra* n. 21, at 2.

28. *See id.*

29. *All Things Considered*, "Robert Siegel Interview: Captain Bob Guidara Discusses the Failure of the Security Surveillance System Tested in Ybor City to Make a Single Positive Identification in Two Years" (Natl. Public Radio Aug. 20, 2003) (news broadcast).

30. *Id.*

31. Natalie Smith, *Putting a Finger on Biometrics*, 7 MOVE Magazine 2 <http://www.aamva.org/products/Move/archive/proPublicationsMOVESummer2002 FingerOnBiometrics.asp> (Summer 2002).

32. *Id.*

33. *Id.*

34. For example, the Director of Information for the West Virginia DMV suggested that the raw numbers are reflective of the amount of fraud deterred:

> Morgan says the facial recognition system is doing a good job of preventing fraud. 'So far, we've refused or denied about 6,000 licenses. When we tell people their photos don't match, they go to the car to 'get something' and they're gone . . . .

See id.

In the aftermath of September 11 terrorist attacks, the American Association of Motor Vehicle Administrators announced plans to require that all drivers' licenses contain a fingerprint or digital photo that could be electronically scanned into a state, cross-jurisdictional database.[35] This is a separate initiative from the federal project to enroll data from foreign visitors described in the opening of the article.

Hand geometry technology creates mathematical pattern abstractions using data derived from the length, width, thickness, curvature, and surface area of the hand and four fingers.[36] The quality of the enrollment image will affect how often the system falsely rejects the individual in the future, and proper enrollment may require that the user learn the feel of the system. For example, users may be told to imagine landing an airplane as they place their hand on the platen.[37] Hand geometry technologies are designed for verification that a person is who they are claiming to be rather than for identification through "one-to-many" matching.[38]

Although less accurate than fingerprints, hand geometry systems are relatively easy to use and, thus, are used more than any biometric system other than fingerprinting.[39] For example, more than 90% of the nation's nuclear facilities use hand geometry readers to validate entry,[40] Disney World uses a two-finger geometry system to verify its season pass holders,[41] and the San Francisco International Airport uses hand geometry to control access to the tarmac.[42]

Eye Scanning is the final biometric technology currently in use. Although eye scanning frequently appears in Hollywood movies with futuristic settings,[43] the technology is far from fictional. Modern

35. *See* Richard Sobel, *The Demeaning of Identity and Personhood in National Identification Systems,* 15 Harv. J. L. & Tech. 319, 328 (2002).

36. Richard L. Zunkel, *Hand Geometry Based Verification*, in *Biometrics: Personal Identification in Networked Society* 87, 89 (Anil K. Jain, et al., eds. 1999).

37. *See id.* at 91.

38. *See id.* at 87.

39. *See* Higgins, *supra* n. 16, at 65, 69.

40. *See* H.R. Subcomm. on Technology, Terrorism, and Govt. Info. of the Senate Comm. on the Judiciary: *Hearing on Biometric Identifiers and the Modern Face of Terror: New Technologies in the Global War on Terrorism:* 107th Cong. 12, 42 (2001) [hereinafter *Biometric Identifiers*] (Statement of Martin Huddart, general Manager, recognition Systems, Inc., Ingersoll-Rand).

41. *See* Higgins, *supra* n. 16, at 67-68.

42. John D. Woodward, *Biometric Scanning, Law & Policy: Identifying the Concerns—Drafting the Biometric Blueprint*, 59 U. Pitt. L. Rev. 97, 106 (1997).

43. *See, e.g., Never Say Never Again* (Warner Brothers 1983) (motion picture); *Mission: Impossible* (Paramount Pictures, 1996) (motion picture); *Charlie's Angels*

technology has offered both iris and retinal scanning, although retinal scanning systems are no longer commercially available.

An iris scan uses an infrared light to identify and create mathematical abstractions of patterns in the colored tissue around the center of the eye.[44] Current commercial iris scanning systems works at a range of about 3 to 7 inches, although some research systems may operate at a range of 5 meters.[45] The verification time can be as fast as 4 seconds in practice.[46] Enrollment in the system is more difficult than enrollment for systems such as fingerprint, face scanning or hand geometry. The eye must be properly positioned and focus held during the scan.[47]

Retinal scanning is similar, but analyzes the patterns of veins occurring in the back of the eye.[48] Both eye scanning techniques deter some types of fraud because it is difficult to change one's iris or retinal patterns, short of the fictional technology depicted in the movie "Minority Report," although other forms of subterfuge may exist[49]

Virgin Atlantic and British Airways use the EyeTicket Jetstream System to rush frequent transatlantic passengers past the passport check.[50] John F. Kennedy International Airport has installed an iris scan system for employee access to restricted areas.[51] In a fascinating use of the iris scan, *National Geographic* took a famous photograph of

(Columbia, 2000) (motion picture); *X-Men* (Twentieth Century Fox, 2000); *Minority Report* (Twentieth Century Fox, 2002) (motion picture).

44. John Daugman, *Iris Recognition*, 89 no. 4 Am. Scientist 1 (Jul.-Aug. 2001); Richard P. Wildes, *Iris Recognition: An Emerging Biometric Technology,* 85 Proceedings of the IEEE 1348 (Sep. 1997).

45. Nicolas Orlans, *Eye Biometrics: Iris and Retina Scanning,* in *Biometrics* 89, 91 (Jane K. Brownlow, ed., 2003).

46. *Id*. at 93-94.

47. *See* Wildes, *supra* n. 44, at 1351, 1353 (noting that the person enrolling must properly position the eye and describing the need to maintain a steady gaze). In addition, some test subjects report discomfort from the light. *See id*. at 1361.

48. Orlans, *supra* n. 45, at 95.

49. *See* John Daugman, *Recognizing Persons by Their Iris Patterns*, in *Biometrics: Personal Identification in Networked Society* 123, 126-27 (Jain, et al., eds. 1999) (describing countermeasures against subterfuge). In addition, disease or injury like hemorrhaging, glaucoma or occlusion may change the patterns. *See* Orlans, *supra* n. 45, at 95.

50. Sean Henahan, *The Eyes Have It* <http://www.accessexcellence.org/WN/SU/SU102001/irisscan.html> (Jun. 17, 2002).

51. Terminal 4 JFK International Airport, *JFK IAT & Port Authority Unveil Iris Scan Security Solution* **<**http://www.jfkiat.com/Documents/Latest%20News_oct/iris%20scan.htm> (accessed Nov. 15, 2003).

an Afghan girl with haunting eyes and used iris scanning to identify the girl 18 years later.[52]

III. Implications of Biometric Technology

Using biometrics, particularly for verification purposes, offers great advantages over current methods in terms of convenience, accuracy and security. Instead of remembering ten passwords and changing them every month, one could simply put a finger on a platen connected to the computer.[53] Instead of harried airline employees squinting at a driver's license photo taken five years and twenty pounds ago, airlines could adopt a biometric measure to more precisely confirm that the person entering the airport or getting on a plane is the person listed in the documents and is not among those considered a security risk. Leaving your driver's license or ATM card at home by mistake would no longer matter because your biometrics measurements are a part of you and go wherever you go.[54]

Biometric technology also is appealing from a security standpoint.[55] Accessing funds from the ATM using a thumbprint instead of a card or password enhances security given that a thief would have a harder time stealing your thumbprint than your ATM card.

There is a temptation, however, to romanticize the security and accuracy of biometric technology. In extolling the virtues of biometrics, for example, Senator Dianne Feinstein declared that biometric identifiers are the most secure and convenient form of authentication because "they cannot be borrowed, stolen, forgotten

52. Henahan, *supra* n. 50; *see also* Cathy Newman, *A Life Revealed*, 201 no. 4 Natl. Geographic 8 (Apr. 2002) (excerpt available at <http://magma.nationalgeographic.com/ngm/afghangirl/>); David Braun, *How They Found National Geographic's "Afghan Girl"*, National Geographic News <http://news.nationalgeographic.com/news/2002/03/0311_020312_sharbat.html> (March 7, 2003) (describing how the National Geographic team located the girl from the photo and verified her identity).

53. Inexpensive devices are available currently to control access to computers through fingerprints. *See Biometrics and the Future of Money, supra* n. 1, at 48 (statement of Oscar R. Pieper, President, Indicator technology) (describing a computer mouse with a fingerprint reader for less than $100).

54. *See id* at 7 (statement of Mr. Dunn). Citibank is already looking into the feasibility of implementing a fingerprint or face scanning system for ATMs. *See* Lucas Mearian, *Toppling the PIN: Banks eye Biometrics for ATM Access* <http://www.computerworld.com/securitytopics/security/story/0,10801,67314,00.html> (Jan. 11, 2002).

55. Nanavati et al., *supra* n. 9, at 4 (2002); Woodward, *supra* n. 42, at 101.

or forged."[56] Despite the glowing praise, biometrics are neither perfectly secure nor perfectly accurate.

No biometric technique is completely accurate.[57] For facial scans, different lighting, background composition, or odd angles may cause a mistake in identification.[58] Eye scans require the eye to be positioned perfectly to avoid an error.[59] Although a finger scan is generally reliable, it may be misread at different angles or pressures.[60] Moreover, the general question of reliability should be broken down more specifically into consideration of false positives and false negatives, given that the policy implications may differ. For example, consider the results of one iris scan system test. In 878 attempts, the system being tested did not once admit someone who was not the person enrolled with the iris scan data. The test, however, produced 89 false rejects, in which the system refused to accept someone who did match the data. From a policy standpoint, the low level of false accepts suggests that the system strongly addresses security concerns by consistently rejecting those who did not belong. On the other hand, the considerable level of false rejects could foreshadow inconvenience, frustration and improper denial of access for many. The question of whether the system is reliable enough to implement may turn on policy choices concerning which goals are paramount and which goals are expendable.

In addition, there has been little testing of the accuracy of many types of biometrics outside laboratory conditions, and it is difficult to create statistically significant trials of sufficient variations in the laboratory.[61] For example, accuracy results of a fingerprint system for a population of elderly people in a dry environment may vary from the accuracy results for a population of young people in a humid environment.[62] Similarly, the accuracy rate of a facial imaging system may vary tremendously when tested against those actively trying to conceal their appearance as opposed to those who are trying to be

56. *See Biometric Identifiers*, *supra* n. 40, at 2 (statement of Sen. Dianne Feinstein).

57. *See* Nanavati et al., *supra* n. 9, at 23-41 (chapter discussion on accuracy in biometric systems); John D. Woodward, Jr. *Searching the FBI's Civil Files: Public Safety v. Civil Liberty,* in *Biometrics* 307, 324 (Jane K. Brownlow, ed., 2003).

58. *See* Nanavati et al., "Factors Affecting False Nonmatch Rates," *supra* n. 9, at 30-31 tbl. 3.1.

59. *Id.*

60. *Id.*

61. *Id.* at 23 (noting that Disney World's use of finger geometry would have been a good real-world study of accuracy, but that the results of that study are classified).

62. Bjorn, *supra* n. 14, at 111.

recognized for access.[63] In a recent demonstration of the problem, *National Geographic* magazine asked a former CIA operative to try to fool a facial imaging system using techniques such as glasses, facial hair and head positioning.[64] When the system tried to match the operative's current photo against various types of disguised images, the level of correlation ranged from roughly 60 percent to 80 percent.[65] The results were even worse when the system tried to make the match using a photograph from 27 years before. In that case, the level of correlation between the old photo and the operative's undisguised face was only 19 percent and the level of correlation between the old photo and various facial disguises ranged from 8 percent to 12 percent.[66]

And finally, the accuracy of any computer system is only as good as the individuals who operate and maintain the system.[67] Human error, undoubtedly, will be an additional source of mistake and confusion.

In addition to the possibility of a mistake, biometric technology cannot eliminate the possibility of fraud. The computers that collect and evaluate biometric information are vulnerable to the same type of fraud and manipulation as other computers.[68] The biometric information housed in the computer could be accessed and erased, altered, or copied. In theory, programs could be written to circumvent the system. Moreover, the fraud need not be based on sophisticated

63. *Id.*

64. Shenk, *supra* n. 23, at 18-19.

65. *See id.* at 19.

66. *See id.*

67. As engineer and social scientist Donald Norman notes, "In the end, security depends upon people. You can have the most powerful encryption in the world, but the weak link is the systems, procedures, and people who implement them." *Don Norman's jnd.org: Recommended Readings* <http://www.jnd.org/recommended_readings.html> (accessed Dec. 1, 2003) (reviewing Bruce Schneier, *Secrets & Lies: Digital Security in a Networked World* (John Wiley & Sons 2000)).

68. Data, of course, can be stolen or misappropriated without sophisticated hacking programs. For example, in November of 2003, a thief who stole a laptop computer also netted the names, addresses, and social security numbers of thousands of Wells Fargo Bank customers. David Lazarus, *A Simple Theft Nets Wells a World of Woe: Break-In Behind Bar Puts Clients' Data at Risk*, San Francisco Chronicle A1 (Nov. 21, 2003), available at <http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2003/11/21/MNGLT37MH71.DTL>. The laptop belonged to an outside consultant working for the bank. *Id.* Similarly, in October of 2003, a woman in Pakistan, who was doing outsourced clerical work for UCSF Medical Center, threatened to release patient files onto the internet unless the hospital helped her collect outstanding funds owed to her by her employer. David Lazarus, *San Francisco Chronicle*, *Pakistani threatened UCSF to get paid, she says* <http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2003/11/12/BUGI52VMQR1.DTL> (Nov. 12, 2003).

computer technology. Crude approaches already exist to manufacture or avoid a fingerprint match.[69] More sophisticated methods of biometrics fraud may develop as the technology becomes more widespread.

The fact that biometrics data can be faked, however, is not a complete indictment of the technology. It is still harder to steal and reproduce your iris scan than it is to steal and reproduce your mother's maiden name.

The real problem is not that biometrics are subject to fraud or error, but our conviction nonetheless in its accuracy. Human beings have an almost blind faith in all things scientific,[70] and biometric data is cloaked in the mantle of scientific truth. Thus, if a computer tells a government agent that a person's retinal scan matches that of a notorious criminal or someone who should be denied access to a building or a plane or a country, it will be very difficult for the person to argue the computer is mistaken. In other words, the problem lies not in the possibility of mistake about who we are, but rather the physical and psychological barriers to challenging a mistake about who we are.[71]

More important, the relevant question may not be who you are, but what you might have done or might do. The ability to accurately identify an individual does not mean that we necessarily know what acts the individual has committed or might commit. The danger is that our belief in our ability to identify people with great accuracy will cloud our judgment about what one has done or what one is likely to

69. European refugees have been known to soak their hands in henna so that their fingerprints will be harder to detect. Moreover, studies have shown thin fingerprint pads adhered to the fingers have managed to fool scanners. *See* Higgins, *supra* n. 16, at 64; *see also* Valorie S. Valencia & Christopher Horn, *Biometric Liveness Testing*, in *Biometrics*, 139, 139-149 (Jane K. Brownlow, ed., McGraw-Hill 2003) (describing anecdotal and lab evidence related to whether fingerprint reading technology can be fooled by something other than a live person's finger on the plate).

70. *Cf.* James L. Wayman, *When Bad Science Leads to Good Law: The Disturbing Irony of the* Daubert *Hearing in the Case of U.S. v. Byron C. Mitchell* <http://www.engr.sjsu.edu/biometrics/publications_daubert.html> (Feb. 2, 2000) (commenting on probability-based arguments that are unfounded and misleading to the jury, and noting that there is a history in American jurisprudence of human identification based on the gross misuse of statistical and probability theory).

71. It is possible that the problem can be traced to our lack of experience with biometrics. Over time and through unpleasant experiences, we could, in theory, develop a healthy suspicion of biometrics. A significant number of individuals, however, could be trampled in the process of our experiential learning.

do.[72] We may transpose our certainty about identity into a certainty about a person's past or future behavior. The difficulty of challenging a false biometric reading and the potential for improper assumptions based on biometric readings are particularly troubling given the settings in which biometrics are likely to be used. Much biometric technology is likely to be used by government agencies in settings such as licensing and access, settings that may not provide the same type of due process protections as criminal investigations. Similarly, the technology may be used for verification and identification of citizens of foreign countries, who are not afforded the same level of rights as U.S. citizens Finally, biometric technology will be used in private commercial settings, in which individuals as a general matter do not enjoy the same types of process rights as they would in relation to government action, short of specific consumer legislation.

In short, despite the greater accuracy and reliability of biometrics than other forms of verification and identification, the technology raises concerns related to the barriers of challenging mistake and fraud as well as the unfortunate potential to make false assumptions based on the biometric results. Assuming we can overcome concerns about inaccuracies, improper assumptions and bias towards things scientific, the use of biometrics also raises concerns of reinforcing societal prejudices and denying fundamental notions of individual identity.[73]

Historically, biologic differences such as race, sex and skin color have been used to categorize people into groups and discriminate against them based on those categories. To the extent that widespread use of biometric technology promotes such categorization, it may contribute to our unfortunate tendency as a society to judge people by including them in biologic groups and making assumptions about those groups. There is a danger that the more we focus on biologic characteristics, the less we remember the intangible aspects of a person's character. As a result, perhaps we should be wary of moving towards a society that constantly reduces us to our biologic characteristics.

As mentioned above, biometrics are merely a form of data. Thus, collection of biometric data raises some of the same issues that arise

72. Problems related to scientific evidence are not confined to biometrics. We already worry about whether juries can distinguish between the accuracy of scientific evidence and whether the evidence proves anything.

73. Sobel, *supra* n. 35, at 320 (arguing that national identification systems transform intrinsic qualities about individuals into numeric designations such that our personhood becomes an attribute of bureaucratic computerized systems).

when government agencies or private firms collect any information about citizens. Such concerns include whether information about a citizen should be afforded some degree of protection under privacy doctrines or doctrines related to freedom of speech and association.[74]

Although other panelists will address issues related to data collection and data mining in general, it is worth noting two issues that relate specifically to collection of biometric data. First, some commentators express concern that biometric data could potentially reveal information about health status.[75] Such concerns are based on the notion, for example, that examining a person's iris or retina could possibly show evidence of various health conditions such as pregnancy or hypertension.[76] Similarly, some researchers have suggested a link between fingerprint patterns and male homosexuality, but the data, as well as the conclusions drawn from the data, are controversial.[77]

It would take a significant technological shift, however, to go from current biometric systems to systems that reveal disease or other health information. As described above, current biometric systems do not operate as a human observer would, but rather translate information into a mathematical construction that has no physiological meaning.[78] Retinal scanning devices, for example, do not take an image of the retina. They scan the retina in a circle to create a one-dimensional pattern.[79] Such abstracted information does not reveal collateral health status.[80]

It is possible that different approaches to biometric technology could develop in the future. In that case, we might need to harmonize rules regarding the collection and use of biometric data with rules regarding the collection and use of health information.[81]

---

74. For an exploration of Constitutional issues related to data collection in general, *see id.* (exploring the implications of a national identification system); Christopher Slobogin, *Symposium: Public Privacy, Camera Surveillance of Public Places and the Right to Anonymity,* 72 Miss. L. J. 213 (2003); *see also* Greg Star, *Airport Security Technology: Is the Use of Biometric Identification Technology Valid Under the Fourth Amendment?*, 20 Temp. Envtl. L. & Tech. J. 251 (2002).

75. *See* Woodward, *supra* n. 42, at 115-117 (1997).

76. *Id.* (quoting Dr. Harold Chen, *Medical Genetics Handbook* 221-226 (1988)).

77. *Id.* at 117.

78. *See supra* nn. 13-16 and associated text.

79. *See* Hill, *supra* n. 15.

80. *See* Orlans, *supra* n. 22, at 98 (noting that retinal scanning is not inherently prone to privacy abuse because a special process called angiography is needed to scan for medical conditions that biometric retinal scanning would not be able to reveal).

81. For example, Congress, with the Amendments to HIPAA, has implemented privacy restrictions that require elaborate consent before health information can be

Second, biometric technology raises for many people the specter of government tracking. It creates the fear that government, by constant collection of biometric data, will be able to monitor substantially all of our movements from day to day.[82] Tracking is no more than data processing, however, and it could be accomplished without biometrics. For example, if individuals are required to enter passwords or social security numbers often enough for computer access, building access, and credit access, and the government has the ability to collate the data, the government could track substantially all of an individual's movements from day to day without ever collecting biometrics.

Biometric data creates an additional level of tracking concern only if the data can be obtained surreptitiously. For example, entering passwords and social security numbers requires a citizen's knowledge and participation to physically enter the information into a data collection device.[83] In theory, information about a person's physiological and behavioral characteristics could be collected without their knowledge or consent. If this were true, such biometric technology could substantially facilitate tracking, beyond the capabilities of other identification technology.

In order to accomplish this, the government would need the capacity to both surreptitiously collect biometric data and scan large data bases for "one-to-many" identification. Current biometric technology lacks the sophistication necessary to facilitate such a process. As described above, only fingerprints and retinal scans have the ability to reliably scan large databases to identify a random individual rather than confirming that an individual is the person claimed.[84] Neither fingerprints nor retinal scans, however, can be

revealed. Jack A. Rovner, Kathryn A. Roe & Ralph L. Glover, *Managing the Privacy Challenge: Compliance with the Amended HIPAA Privacy Rule*, 15 Health Law 18 (2002). These restrictions apply to health insurers, providers, employers engaged in facilitating health insurance, and related parties. *See id.* at 21 (describing covered entities and citing 45 C.F.R. §160.103). If it were true that health information could be collected, revealed and distributed along with biometric data, such regulations could be undermined.

82. *See, e.g.,* Nguyen, *supra* n. 21, at 4 (noting we are uneasy at having police officers using technology so powerful that it approaches Big Brother's omnipresence and omniscience).

83. One could argue that even if biometrics must be collected with knowledge and consent, biometrics is still more troubling as a tracking device than data such as Social Security numbers. Society is accustomed to recognizing that Social Security numbers can be wrong, and more likely to accept biometric data on faith.

84. *See supra* n. 12 and associated text.

collected without a party's consent and participation, at least not in the manner necessary to facilitate large-scale tracking.[85]

It is also possible that non-biometric technology could advance towards allowing surreptitious tracking sooner than biometric technology. For example, product manufacturers, the Defense Department, and retailers such as Wal-Mart are in the process of implementing product tracking systems using tags that send radio signals.[86] Unlike the familiar bar codes, the tags do not need to be scanned at close range. A commercial version without a power source can be read from 20 feet away, while a defense department version with a power source linked to global positioning satellites can engage in remote tracking.[87] Such tracking systems potentially allow government or industry to monitor the location of products without telling the person wearing or holding the product that it is being monitored. In addition, for tags with a power source, monitoring could continue after the product has left the store. The tags are intended as inventory tracking devices, and industry users are currently focusing on tagging pallets and cartons of products rather than tagging individual items.[88] Nevertheless, the tags raise the potential of surreptitious tracking through items worn or possessed by individuals without the use of any biometric information.[89]

In sum, current biometric technology does not have the capacity to allow large scale tracking, and large scale tracking may be feasible through non-biometric measures sooner than through biometrics. Nevertheless, the potential for the technology to develop towards large scale tracking in the future raises concerns about the ways in which government or industry could use the information collected, if such potential were realized.

85. In some circumstances, fingerprints can be collected surreptitiously by removing items that an individual has touched. The process, however, does not work in all circumstances and would not facilitate the type of tracking contemplated in the Orwellian vision.

86. *See* Barry J. Feder, *That Needle Hopelessly Lost in the Haystack*, N.Y. Times C1 (Sep. 29, 2003).

87. *See id.*

88. *See id.*

89. Privacy advocates have suggested protections such as requiring that products with embedded tags carry warning labels, that the tags be designed so that they cannot be reactivated once turned off, and that the tags must be removed unless the buyer agrees to leave it on. *See id.* In a more familiar example, cell phone usage can provide surreptitious information about a person's movements.

IV. Looking Forward

One theory of the origin of the word "sabotage" suggests that workers during the Industrial Revolution threw their shoes (sabots) into the machines in hopes of preventing the march of technology that was threatening their jobs.[90] The effort failed, however, and the Industrial Revolution continued.

It is always difficult to turn back the tide of technology, and I suspect one would be no more successful at preventing the use of biometric technology than the workers were at sabotaging the machines. We can, however, attempt to impose parameters on the use of biometrics, parameters that may protect an individual's interest in the accuracy and appropriate use of biometric information. The limitations are particularly important to think through before the use of the technology is fully entrenched because it may be easier to channel behavior before it becomes habituated in particular directions.

Biometric information currently is collected by numerous private and public entities operating under varying types of regulation or lack thereof. Although it could be useful to standardize requirements across these disparate circumstances, such a comprehensive approach is unlikely to occur, particularly not in the short term.[91] Nevertheless, current developments in the implementation of biometric technology offer a tantalizing opportunity to influence the use and even the development of biometrics.[92] Governmental projects involving widespread implementation of biometrics provide a vehicle for establishing benchmark standards. Approaches chosen now may set the stage, not only for the rules that apply to governmental use of

90. David Wilton, *Etymologies & Word Origins: Letter S* <http://www.wordorigins.org/wordors.htm> (last updated Jun. 27, 2003).

91. As a comparison, statutory protections concerning the privacy of data about an individual have not proceeded in a comprehensive fashion in the United States. The statutes that do exist have tended to focus on the public sector. In contrast, European efforts have focused on the public and private sectors as a whole. *See* Stephen R. Salbu, *The European Union Data Privacy Directive & International Relations*, 35 Vand. J. Transnatl. L. 655, 666 (2002). Where regulations do exist in the United States concerning industry use and collection of data about individuals, such regulations tend to be focused on particular industries, such as the financial industry, the credit reporting industry, or the health care industry. *See id.* at 667; *see also* Rovner, et al, *supra* n. 81 (describing the amended federal HIPAA rules).

92. *See e.g., supra* text accompanying nn. 2-5 (describing implementation of biometric technology at all U.S. points of entry); *supra* text accompanying n. 35 (describing coordinated effort of state motor vehicle departments to require biometrics for driver's licenses).

biometrics in the future, but also for rules that private commercial entities may implement or that Congress may impose on them.

Most important, given the purchasing power of the government, the paths chosen today have the potential to affect how the technology develops. The government as consumer will express its wishes to the technology suppliers who will attempt to develop the technology along those lines. This in turn affects our understanding of what is technologically possible and the choice of rules we can implement.

Much of the discussion of implementing biometrics revolves around establishing standards for the reliability of a given technology and for protection of the data from fraud or misappropriation.[93] I would categorize these efforts as attempts to prevent mistake, fraud and abuse before the fact. Despite the obvious value of such initiatives, this should not be our only concern. No matter how much we invest in prevention of mistake, fraud and abuse, no system is foolproof. Mistakes will occur, either through technological or human error. Biometric information will be fraudulently used or altered. And government agents, intentionally or inadvertently, will violate whatever rules we establish limiting the use of the biometric information. Thus, substantial efforts also should be directed at establishing methods to review and challenge biometric determinations.

A. Giving Individuals the Opportunity to Review and Challenge Biometric Determinations

An individual's interest in ensuring the accuracy and proper use of personal biometric information is unlikely to be fully represented by other actors in the system. Although one might expect that government or private organizations would be as interested in reliable determinations as the individuals who are tested, the interests may diverge. For example, an organization may use biometric

93. *See, e.g., Biometric Identification and the Financial Services Industry, Hearings Before the House Subcomm. on Domestic and Intl. Monetary Policy of Comm. of Banking and Financial Services*, 105th Cong. (May 20, 1998); H.R. Subcomm. on Technology, Terrorism, and Govt. Info. of the Senate Comm. on the Judiciary: *Hearing on Biometric Identifiers and the Modern Face of Terror: New Technologies in the Global War on Terrorism:* 107th Cong. 12, 42 (2001); Jain et al., *supra* n. 8; John D. Woodward, *Biometrics: Privacy's Foe or Privacy's Friend?*, in *Biometrics: Personal Identification in Networked Society* 1487 (Anil K. Jain, et al., eds. 1999); Weicheng Shen, Marc Surette, & Rajiv Khanna, *Evaluation of Automated Biometrics-Based Identification and Verification Systems*, in *Biometrics: Personal Identification in Networked Society* 1487 (Anil K. Jain et al., eds. 1999); *see also* Star, *supra* n. 74, at 7-8; Nguyen, *supra* n. 21.

technology, but have very little interest in its reliability. Consider an organization that requires individuals to put their fingerprint on a personal check used to purchase traveler's checks. If a fraud allegation arises, the organization can give the check to the police to help track down the suspect.[94] The organization could decide that the main value of collecting the biometric lies in the system's ability to scare off potential defrauders. In other words, those planning to defraud the organization will see the fingerprint requirement and choose to perpetrate their fraud elsewhere.

If the main goal is deterrence, rather than confirming the identity of those who cash checks, the organization could rationally choose to purchase inexpensive equipment with a low level of reliability. In that case, the interests of the organization and the individual would not converge. Individuals would be much more interested in the reliability of the equipment, given that they must bear the burden of straightening out errors that occurs. Although the testing entity will have to invest some time in the mistakes that occur, the potential damage and resulting burden to the individual of being improperly investigated by the criminal system are far greater than any burden the testing entity will bear.

In fact, an individual normally will have a greater interest than the government or other testing entity in ensuring that his information is accurate. This would be true almost regardless of the entity's level of interest in the accuracy of its determination. For example, although the testing entity may be willing to tolerate a mistake related to one person out of a thousand, that one person is likely to have a zero tolerance for mistakes related to himself.

Given the divergence of interests, individuals should have the ability to serve as watchdogs for their own information to confirm its accuracy and appropriate use. In particular, procedures should be established allowing individuals to periodically check and correct their biometric information in the same way that individuals can check and correct their credit status.[95] Although lay people currently do not have the ability to analyze raw biometric data and its implications, if access were granted, one would expect a market to develop in products or services designed for this purpose.

94. The California State Automobile Association currently has such a procedure.

95. Procedures for correcting inaccuracies detected through periodic review could follow the path outlined below for general rules for challenging biometrics. *See infra* text accompanying nn. 113-15.

The greater challenge will be to delineate procedures for individuals who wish to challenge a biometric determination made in the course of a denial of rights or privileges. Such a challenge could take the form of arguing that the biometric is inaccurate or that the conclusions drawn from the biometric are inaccurate.

As described above, biometric determinations raise greater concerns than other forms of identification in light of our potential to blindly accept the accuracy of the information and discount the possibility of error, as well as the danger that we will transpose this certainty about identification into certainty about a person's past or future behavior. Given the difficulty of challenging information cloaked in the mantle of scientific truth, one could argue that the governmental agency should bear the burden of proving the accuracy of its determination, rather than the individual bearing the burden to prove that the information is wrong. This is consistent with the fact that, as between the agency and the individual, the agency has better access to the information that would determine whether inaccuracies exist. Nevertheless, insisting that government agencies shoulder the burden of proving the accuracy of every biometric determination could result in a crushing administrative burden and interfere with the legitimate exercise of governmental interests. The goal will be to balance these competing interests in the context of government action based on biometrics.

An individual's right to challenge government action generally is governed by due process doctrines. The Fifth and Fourteenth Amendments require that government shall not deprive an individual of liberty or property without due process of law. Thus, the question for biometric determinations will be whether the resulting government action constitutes a deprivation of liberty or property and, if so, what process is due.

The notion of a deprivation of liberty is not limited to the types of formal constraints imposed by the criminal process.[96] Although incarceration may be an extreme form of deprivation of liberty, the Supreme Court has found liberty interests implicated when government action may harm an individual's standing and reputation in the community. For example, in *Joint Anti-Fascist Refugee Committee v. McGrath* (1951), the Court found a liberty interest involved in the federal government's designation of certain organizations as "Communist."[97] Similarly, in *Wisconsin v.*

96. *Board of Regents of State Colleges v. Roth*, 408 U.S. 564, 572 (1972).

97. *Joint Anti-Fascist Refugee Committee v. McGrath*, 341 U.S. 123 (1951).

Constantineau (1971), the Court found a liberty interest involved in an ordinance providing that local police could publicly distribute lists of individuals not permitted to purchase alcohol.[98]

Due process doctrines, however, do not prevent the government from acting whenever the action may harm an individual's liberty interest. Rather, deprivation of a liberty interest brings to bear the requirement that the governmental body act according to appropriate procedures and afford the individual an opportunity to be heard and to challenge the government's determination.[99] In addition, in at least one case involving deprivation of liberty interests, the Supreme Court construed due process as requiring notice and an opportunity to be heard prior to the government's action.[100]

Analogous to deprivations of liberty, the notion of a deprivation of property is not limited to traditional notions of land or tangible items confiscated by the government. The Supreme Court has found property interests implicated in termination of government privileges such as disability benefits and welfare payments.[101]

Unlike deprivation of liberty, however, deprivation of a property interest does not necessarily require notice and an opportunity to be heard prior to the deprivation. Thus, in *Mathews v. Eldridge*, the Supreme Court found no pre-termination hearing necessary for termination of the complainant's disability benefits.[102] The *Eldridge* Court based its determination on consideration of 3 factors: 1) the private interest that would be affected by the official action; 2) the risk of an erroneous deprivation of the interest and the value of any additional safeguards; and 3) the government's interest in the function involved, including the fiscal and administrative burdens that additional procedures would create.[103]

Logic from the liberty and property lines of cases may suggest a framework for challenges to biometric determinations by government

98. *Wisconsin v. Constantineau*, 400 U.S. 433 (1971).

99. For the federal government, modern due process requirements are grounded in statutory law as well as constitutional law. *See* 5 U.S.C. § 556 (2000).

100. *See Constantineau*, 400 U.S. at 437 (finding that when a person's good name, reputation, honor or integrity is at stake because of what the government is doing to him, notice and an opportunity to be heard are essential).

101. *Mathews v. Eldridge*, 424 U.S. 319 (1976); *Goldberg v. Kelly*, 397 U.S. 254, 263 (1970).

102. *Eldridge,* 424 U.S. at 319. (arguably the high water mark of due process rights for termination of government benefits, the Supreme Court did require a pre-termination hearing, although the Court explained that the requirement could be satisfied by something short of a full judicial inquiry) *See Goldberg*, 397 U.S. at 266-67.

103. *See Eldridge*, 424 U.S. at 321.

entities. Consider, for example, an individual traveler moving through the security line at the San Francisco airport. The traveler's biometric is scanned and matched to relevant travel documents and to the government database. Suppose the traveler is informed that he will not be allowed to board the plane. What procedures should exist to challenge the biometric determination?

Answering the question begins with identifying the type of interests the disappointed traveler can claim and considering the strength of those interests in comparison to ones that have been protected as liberty or property interests. The disappointed traveler may be able to argue that the government's action implicates a liberty interest by damaging his reputation and standing in the community. Family members and business associates traveling with him will know of the government's refusal to allow the traveler on the plane. They may reasonably infer that the government believes this person represents an unacceptable risk of some kind, a judgment that may affect their willingness to trust and associate with the traveler.[104]

The government's action, however, is less intrusive into the traveler's standing in the community than the government actions in the liberty cases that involve posting lists for public consumption.[105] In particular, the traveler's information is not trumpeted to the community at large. Although those who receive the information by incidental contact may make assumptions that are damaging to the individual's reputation, if the government does not publicly announce a damaging reason for the denial,[106] bystanders are free to draw less

104. The traveler potentially could claim deprivation of a property interest on the grounds that he is denied the ability to exercise the value of his plane ticket. Given that the amount of process due may depend on the type of interest and the strength of that interest, however, the property claim would be considerably weaker than the deprivation of liberty claim. One would imagine that the process due for the loss of a plane ticket would be less than the process due for the loss of reputation.

105. The *McGrath* and *Constantineau* cases both involved public postings of information. In *Constantineau*, the chief of police distributed a list of names to liquor store owners noting that those individuals should not be allowed to purchase alcohol. 400 U.S. at 433. In *McGrath*, the organizations' names were published in the federal register. *341* U.S. at 129 n. 3. One could argue, however, that the McGrath case concerned less than public posting. The publication in the Federal Register included the names of the organizations rather than the members of the organization. The list containing individual names, however, was distributed to public agencies and departments for the purposes of denying employment. From this perspective, the *McGrath* "no-employment" list distributed to agencies involved in government hiring could be analogized to a "no-fly" list distributed to agencies involved in airport security.

106. Drawing the line based on the level of public disclosure presents some difficulties. For example, the traveler will undoubtedly want to know the reason for the denial. From a policy standpoint, we would want the government to provide information so that the

damaging conclusions, such as expiration of documents or ticketing problems.[107]

Nevertheless, in all likelihood, the denial of access will have a practical effect on the traveler's reputation. Those who know of the denial are likely to assume the worst. In addition, once the traveler knows he will be rejected, it will be difficult to conceal his "no-fly" status from friends and business associates in the future. There are only a limited number of excuses one can offer for an inability to travel by plane. Thus, denial of access to the plane may affect the traveler's standing in the community, thereby implicating a liberty interest.

The traveler also could argue that he has a liberty interest in moving throughout the country. Denial of access to the plane may implicate his freedom of movement, which could be interpreted as a deprivation of liberty. Again, the fact that the government action implicates a liberty interest would not prevent the government from acting in this manner,[108] but could suggest that process rights may attach, depending on issues such as the nature of the interest involved, the competing governmental interest, and a comparison of the potential benefit to be gained by adding more procedures verses the fiscal and administrative burden of those procedures.[109]

The governmental interest in applying biometric technology will vary according to the use for which the information is intended. In evaluating the strength of the interest for the purposes of identifying a proper review process, however, it is important to consider the risk that the review process will lead to a mistaken result in favor of the

traveler can challenge inaccuracies. The goal of due process is to allow an individual to have notice and an opportunity to be heard. One cannot effectively be heard if one has no idea of the reason for the denial. This, however, poses a dilemma for the government. First, we tell the government to provide information on the reason for the denial. Next, we tell the government that if it provides information on the reason for the denial, it will be branding the individual in the eyes of the community, thereby giving the government an incentive to provide no information at the time of the denial. The clash of dictates could produce an odd dance in which the security agent refuses to speak and insists on silently thrusting legal documents at the traveler. Alternatively, the traveler could end up having to waive his rights in order to receive the information.

107. *Cf. Roth*, 408 U.S. at 573 (declining to find a liberty interest in a case in which the government did not rehire the claimant on the grounds that the state did not make any charge against him that might seriously damage his standing and associations in the community).

108. The government has the legitimate power to restrict movement in many ways ranging from traffic laws that slightly restrict movement to laws of incarceration that drastically restrict movement.

109. *McGrath,* 341 U.S. 123 at 163 (liberty case); *Eldridge*, 424 U.S. at 321 (property case).

individual. Just as biometrics are fallible, so are review processes. Both processes may make mistakes in favor of the individual as well as against the individual. In designating a review system, one must consider the potential harm if the review process reaches a mistaken result in favor of the individual.

In the case of immediate access to an airplane, the potential harm is great. As exemplified by the events of September 11, a small number of individuals with access to a commercial airliner can cause astounding destruction. Although the likelihood is small that any individual traveler boarding a plane poses a threat, the magnitude of the harm is great in those rare circumstances in which the individual does pose a threat.

The magnitude of the potential harm suggests a strong governmental interest. Nevertheless, the problem remains that the data may be wrong or the assumptions drawn from the underlying data may be incorrect. Thus, even in circumstances that present more extreme examples of security considerations, individuals will need the opportunity to challenge the determination. The more difficult questions concern the type of challenge that should be permitted and whether that challenge must occur before the deprivation. In other words, must the government give the traveler a hearing before the traveler can be denied access to the plane or will a post-deprivation hearing suffice?

The question can be framed in terms of a cost/benefit analysis. If one were to require a pre-deprivation hearing, how much error avoidance would be gained and at what administrative cost? A small amount of error avoidance, for example, at a great administrative cost would be unappealing.

It would be difficult to design an effective pre-deprivation hearing for the traveler. Suppose the facial imaging system identifies the traveler as Joe Smith, but the traveler says, "I am not Joe Smith." For an effective hearing, one would need to gather and evaluate a wide range of information, much of which would not be readily available at the airport. For example, if the traveler is not Joe Smith, reasons for the error could include 1) an error by the person who entered the original data about Joe Smith; 2) a programming error; 3) the natural error rate of the technology; 4) fraud in the system or 5) other possible computer or human errors. None of these problems could be efficiently investigated at the airport, particularly not before the scheduled departure time.

The inquiry would be even more difficult if the traveler acknowledges that he is Joe Smith but challenges the government's

determination that he should be denied access to the plane. The information leading to the government's determination could be subject to procedures to protect secrecy and confidentiality. It would be difficult to keep such procedures in place while exploring the accuracy and validity of the government's determination in a short time period. Moreover, a measured evaluation of the validity of the government's judgment would be difficult to accomplish under tight time constraints.[110]

One could argue that the burden of the tight time constraints should fall on the government rather than the individual. If the government cannot adequately make its case during the short time period, the individual should be allowed to fly, and the government could proceed with a fuller inquiry at a later time. This, however, would produce a policy of "fly now, ask questions later," which would be decidedly ineffective against suicide bombers. Again, the magnitude of the potential harm weighs in favor of greater latitude for the government at the moment of departure.[111]

Thus, a pre-deprivation hearing would encounter extraordinarily difficult problems. The time is short, the necessary information is not readily available, and the public safety danger is great. This makes it difficult to design an effective pre-deprivation hearing that would buy

110. One could also argue that a proper hearing would have advocates on both sides. It would be unrealistic to expect that travelers and security agents could summon lawyers to the airport at a moment's notice. In theory, one could grant the traveler the right at the time of departure to require that the government show that it has followed proper procedures in making the determination without requiring the government to reveal any information relied upon. This would grant the traveler a limited pre-deprivation right that could be coupled with the right for a more extensive challenge at a later time. Such a due process right, however, is unlikely to provide much benefit to the traveler, other than to help ensure that the government actually has a procedure for making determinations. One would expect, however, that post-deprivation review would suffice to give the government the proper incentive for establishing reasonable procedures and that such a pre-deprivation right would add little benefit.

111. One could argue that the time limitation problems could be solved by requiring the government to notify individuals who will be designated for additional security or denied access altogether. Prior notification could theoretically allow time for a more leisurely inquiry into the adequacy of the determination. The administrative burden of an effective system of notification would be great. It would require the government to collect and track current address information on the legions of travelers who come through the system. Ironically, although this requirement might appear to be directed at protecting individual rights, it would raise libertarian concerns by mandating increased government tracking and data collection. In addition, many of the individuals will be foreign visitors, greatly complicating the task. One could require only that the government make some effort at notification, allowing notification by publication, for example. Such notification would be fairly ineffective as a method of truly notifying the individuals implicated. Thus, although the latter approach would lower administrative costs, the amount of error correction would be low.

much error avoidance, particularly one that would not impose an unreasonably high administrative burden.

One could argue that a full-blown hearing is not necessary, at least in cases in which the traveler denies that he is Joe Smith. Perhaps the traveler should at least be entitled to display documents contradicting the determination that he is Joe Smith and on that basis, board the plane. A key advantage of biometrics, however, is that they are more difficult to falsify than documents. It would undermine the purpose of biometrics to allow a biometric determination to be overturned on the spot by less trustworthy documents. Those documents, nevertheless, could form the basis of a challenge to the biometric determination in a less time-sensitive and more complete forum at a later time.

The disappointed traveler hypothetical is drawn broadly and simply. In an alternative scenario, an individual already in this country is not denied access to a plane but is designated for additional security reviews. Under those circumstances, the government action may implicate Fourth Amendment protections related to government search and seizure, an issue outside the scope of this article.[112] In addition to potential Fourth Amendment issues, however, designation for additional security review could still implicate liberty interests on the grounds that increased scrutiny creates harm to reputation. If an individual is repeatedly subjected to security reviews, friends and colleagues who witness the heightened security or hear about it may regard the traveler with suspicion and avoid personal or business association.[113]

In sum, the case of the disappointed traveler falls somewhere between the government entitlement cases and the deprivation of liberty cases. The possibility that the traveler is branded as presenting a risk to a civilized traveling society may give the traveler a liberty interest, stronger than the quasi-property interest held by an individual who merely seeks access to a government benefit or privilege. Nevertheless, the potential harm from allowing improper airport access is great, making the government interest quite strong.

112. For discussions of biometrics and the Fourth Amendment, see Slobogin, *supra* n. 74; Nguyen, *supra* n. 21; Star, *supra* n. 74.

113. One could argue that with a proper search, the government need never deny access. Suppose, for example, that an individual agrees to allow an extensive search of his person and luggage. If nothing dangerous is revealed, perhaps the government's concern for potential harm should be fully satisfied. The government could respond, however, that it can never fully anticipate the next generation of weapons and the next wave of threats. Moreover, the government's inability to keep weapons out of jails despite extensive and intrusive searches, casts doubt on the notion that a search can be fully adequate.

The magnitude of the danger and efficiency limitations suggest that an individual's right to challenge the determination at the time of the denial may not be great, although the individual may retain an interest in challenging the determination in a more measured forum after the fact.[114]

An important part of the solution will lie in a careful calibration of the burdens at the subsequent hearing. While we may wish to avoid imposing an overwhelming administrative burden on the government, the government is in the better position to access information about biometric inaccuracies and enjoys the psychological advantage of a presumption of accuracy. We may therefore wish to place an initial burden on the individual to make a limited showing of mistake or inadequacy of a biometric determination with the burden shifting to the government to prove the adequacy of its conclusions.

As a general matter, the proper process for challenging a biometric determination will vary based on the nature and circumstances of the denial. Nevertheless, parameters that emerge from the example of the disappointed traveler may suggest rules for challenging biometric determinations made in a variety of circumstances. First, it will be important to provide an effective opportunity to challenge government denials based on biometrics, although the opportunity need not necessarily occur prior to the denial. This approach would respect both the individual's interest in the accuracy and proper use of his biometric information as well as the government's interest in immediate security. Second, placing the initial burden on the individual and then shifting the burden to the government may strike a balance between the individual's disadvantages in the system of biometric determinations and the need for administrative efficiency.[115]

114. *Cf. North American Cold Storage Co. v. Chicago*, 211 U.S. 306 (1908) (no pre-deprivation hearing necessary for destruction of potentially tainted meat given public health and safety concerns).

115. The rules outlined for due process in challenging biometric information could also be considered for challenging government identification and verification data in general. The bias towards scientific evidence, however, would weigh less heavily in the general data cases, which might affect the allocation of the burdens or the level of the burden applied.

B. Representing the Interests of the Individual in Developing Governmental Policies

As described above, current initiatives offer an important opportunity for shaping the rules that will govern biometric technology far into the future. For the protection of individual interests, it will be important to ensure that individuals are properly represented in the administrative process that leads to implementation of the biometric technology and the development of rules for its use. One cannot reasonably expect government agencies to fully represent the interests of the individual for several reasons. First, policy making may be biased in favor of concentrated interests. Such concentrated interests, including those who create and market the technology as well as private commercial entities that use biometrics, may overshadow the interests of the individual. More importantly, government agencies are themselves stakeholders in the process. They are both consumers of biometric products and implementers of biometric determinations. As such, the agencies will have their own biases based on their potential needs.

In response to this problem, governmental groups designated to choose biometric technologies and implement rules for biometric determinations ideally should include those who can fully represent the interests of the individual. The need is not necessarily satisfied by the inclusion of academics. For example, academics in fields related to developing biometrics technology will be well-suited to consultation on evaluating technology and minimizing the risk of error. Representatives of consumer groups, however, may be better suited for consultation on the rules for limiting the damage from the inevitable errors.

V. Conclusion

Biometric technology promises a revolution in the level of convenience, accuracy and security of personal identification and verification. As we embrace the technology, however, we should pause to consider some of the implications of its widespread implementation. Despite the remarkable level of improvement, the results are still subject to error, both through mistake as well as fraud or abuse. The greatest concern, however, is not the potential for error but rather society's potential reluctance to accept the possibility of error and the resulting barriers for those who are incorrectly identified. In light of these concerns, we should direct attention not only at preventing fraud, mistake, and abuse before the fact, but also

at establishing methods to detect their inevitable occurrence and to limit the resulting damage. To this end, we should take this opportunity to ensure that individuals have adequate procedures for challenging biometric determinations and that individual interests are well represented in the development of governmental policies surrounding biometrics.