Michigan Telecommunications and Technology Law Review

Volume 13 | Issue 2

2007

Biometrics: Weighing Convenience and National Security against Your Privacy

Lauren D. Adkins
University of Michigan Law School

NOTE

BIOMETRICS: WEIGHING CONVENIENCE AND NATIONAL SECURITY AGAINST YOUR PRIVACY

*Lauren D. Adkins**

Cite as: Lauren D. Adkins, *Biometrics: Weighing Convenience and National Security Against Your Privacy*, 13 MICH. TELECOMM. TECH. L. REV. 541 (2007), *available at* http://www.mttlr.org/volthirteen/adkins.pdf

I. WHAT IS BIOMETICS? 542
A. *Finger Prints* 542
B. *Facial Recognition* 543
C. *Hand Geometry* 544
D. *Eye-Based Approaches* 545
II. WHY USE BIOMETRICS? 546
A. *Increased Globalization* 546
B. *The Dangers of the Internet* 546
III. THE RISKS OF BIOMETRICS 547
A. *Technological Advances and the Shrinking Right to Privacy* 548
B. *Biometrics As Applied to* Terry *Stops* 548
C. *Adapting Biometric Systems to Meet Fourth Amendment Requirements* 551
IV. CABINING BIOMETRICS 554
CONCLUSION 555

At Mineta San Jose International, frequent flyers increasingly rely on the Clear system for speedy passage through security checkpoints. In New York, cutting edge technology is used to track city employees when they enter or exit the workplace. Consumers in Indiana pay for their groceries with similar technology and throughout the country, school districts are utilizing recent advances to allow students to pay for lunch, track school buses and parent volunteers and check out library books. Biometrics are not just our future, they are our present. In the wake of 9/11, interest in using biometrics for identity verification has increased. Biometric systems measure physical or behavioral characteristics to identify a person. Particular interest has focused on the areas of visa and

* J.D., expected May 2007, the University of Michigan Law School; B.A., English, Government, Dartmouth College.

immigration documentation and government-issued identification card programs. Biometrics are appealing to security experts because they are closely bound to an individual, are supposedly more reliable, and are difficult to forget, lose, or falsify.

The biometric identifier relies on an individual's unique biological information such as a hand, iris, fingerprint, facial or voice print. When used for verification purposes, a "one-to-one" match is generated in under one second. Biometric technology can substantially improve national security by identifying and verifying individuals in a number of different contexts, providing security in ways that exceed current identification technology and limiting access to areas where security breaches are especially high, such as airport tarmacs and critical infrastructure facilities. At the same time, a legitimate public concern exists concerning the misuse of biometric technology to invade or violate personal privacy.

I. WHAT IS BIOMETICS?

A. *Finger Prints*

Biometrics is the measuring of physical or behavioral characteristics to verify a person's identity.[1] As John Moore notes in "Sensing the Future of Security", fingerprints are the "oldest and most widely used biometric identifier."[2] Once the image is scanned, it is scoured for unique features and stored as a mathematical template. Next, a matching algorithm is stored to compare the template with subsequent fingerprint scans. Law enforcement officials rely upon a score indicating the closeness of the presented biometric to the stored template using the help of a predefined number or algorithm to determine whether the images are sufficiently close enough to be considered a match. There are two forms of fingerprint scans:

The first is an automated fingerprint identification system where responses are generated in minutes. With this method, police conduct a search using an arrestee's fingerprint or a latent print collected at a crime scene against a fingerprint database. One example of this method is the Federal Bureau of Investigation's (FBI) Integrated Automated Fingerprint Identification System (IAFIS), which is a national fingerprint and

1. John Moore, The E-Gov Institute, *Sensing the Future of Security*, June 23, 2003, http://www.fcw.com/fcw/articles/2003/0623/cov-report1-06-23-03.asp.

2. *Id.*

criminal history database.[3] It is the largest ten print system in the world.[4]

The second system is a finger scan. The scan creates an initial template that is then compared against subsequent scans. This method authenticates a person's identity and can be used to control access to facilities, computer networks, and individual computing devices.

In the 1990s, fingerprints were the standard used by law enforcement officials. Much of the attention was given to shifting from ink and paper to livescan and electronic submissions. Government funding focused on aiding law enforcement and border control agencies.[5] Today, there is some concern that manual laborers, those with worn finger pads, individuals born with unreadable fingerprints, and those with unusually dry or moist hands will not be able to participate in automated fingerprinting and scanning systems.[6]

B. *Facial Recognition*

Facial recognition systems rely on images captured from video and digital photos and compare the captured image to those stored in a database. Currently, such systems are being used to locate missing children, limit passport fraud, and combat identity theft.[7] There are two approaches used for facial recognition: feature-based and view-based systems.[8] Again, the images are converted to templates and local feature analysis generates a faceprint. The characteristics of a face (eigenfaces or principal components) are translated into a unique set of numbers using the eigenface method. However, many different algorithms are generated using the various recognition systems. The three most prevalent ones are: principal components analysis (PCA), Linear Discriminant Analysis (LDA) and Elastic Bunch Graph Matching (EBGM). The PCA

---

3. Federal Bureau of Investigation, CJIS Division, Integrated Automated Fingerprint Identification System, http://www.fbi.gov/hq/cjisd/iafis.htm (last visited March 8, 2007).

4. ROBERT F. DIEGELMAN, LOCKHEED MARTIN, LOCKHEED MARTIN BIOMETRICS: THE PAST, THE PRESENT, THE FUTURE (2005), http://www.biometrics.org/bc2005/Presentations/Conference/1%20Monday%20September%2019/Mon_Ballroom%20B/RobertDiegelman.LockheedMartin.pdf.

5. *Id.*

6. Those who are studying biometric modalities and their various applications recognize that one weakness of using fingerprint-based identification verification methods is that such systems will not detect the unique features of a manual laborer's fingerprints due to their worn finger pads, affecting their reliability. Ideally, any biometric system would allow for the universal enrollment of every member of society. PERSONAL VERIFICATION USING PALMPRINT AND HAND GEOMETRY BIOMETRIC, at 1, http://biometrics.cse.msu.edu/Publications/Multibiometrics/Kumaretal_PalmprintHandFusion_AVBPA2003.pdf (last visited Mar. 23, 2007).

7. COMM. ON TECH., NAT'L SCI. AND TECH. COUNCIL, FACE RECOGNITION, at 2, http://www.biometrics.gov/Docs/facerec.pdf (last visited Jan. 31, 2007).

8. *Id.*

method uses eigenfaces to decompose facial structure. The LDA method is a statistical approach and classifies samples of unknown classes, based upon training samples, with known classes.[9] The goal of this method is to maximize between-class variance (i.e. cross users) and minimize within-class (i.e. within user) variance. Using the EBGM approach, the face is transposed onto an elastic grid. A Gabor filter is used to detect shapes and extract features using image processing and recognition is based on the similarity of the Gabor filter response at each Gabor node.[10] One benefit of this biometric system is that it can be used for both identification and verification purposes and can compare live and static images with stored images. However, factors including lighting, expression, and pose can alter the accuracy of these methods.

C. *Hand Geometry*

Similar to fingerprint and facial recognition systems, hand geometry measures characteristics such as length, width, and surface area to develop a template of an individual's hand.[11] To capture these features the hand is scanned using a digital camera. Typically three images of the hand are taken and then evaluated and measured to create a template. When an individual's identity must be verified, the template associated with that person is recalled and the hand is again placed on a plate where the image is taken and a verification template is created.[12] The two templates are then compared and a similarity score is produced and either accepted or rejected, depending on the threshold previously established.[13]

Although it can easily be integrated with other biometric modalities, its use is limited to identity verification only, as a result of its limited accuracy.[14] Another downside is the system's inability to distinguish between a "living" hand and a "non-living" hand, another rationale for limiting the use of such systems to medium-security locales. In addition to identity verification, this system is used to monitor attendance, and restrict physical access. Despite these drawbacks, such systems are generally deemed more acceptable in the eyes of the public since hand scans are perceived as being less invasive.

---

9. *Id.*

10. A Gabor node is a node on the elastic grid that describes the image behavior around a given pixel. *See* COMM. ON TECH., *supra* note 7, at 4 fig. 4.

11. *See generally* COMM. ON TECH., NAT'L SCI. AND TECH. COUNCIL, HAND GEOMETRY, http://www.biometrics.gov/Docs/handgeometry.pdf (last visited Jan. 31, 2007).

12. *Id.*

13. *Id.*

14. CTRS. FOR UNIFIED BIOMETRICS AND SENSORS, UNIV. AT BUFFALO, HAND GEOMETRY BIOMETRICS, http://www.cubs.buffalo.edu/handgeometry.shtml (last visited Jan. 31, 2007).

D. *Eye-Based Approaches*

Iris recognition and retinal scanning are the traditional approaches for eye-based biometrics. Iris recognition captures an image of the iris and stores a record of the iris pattern. This automated system is fairly new and government officials are eager to use this system due in large part to the fact that the details of iris patterns are unique.[15] With this method, the iris is located using landmark features. One difficulty associated with this system is the disruption caused by pupils, eyelashes, eyelids, and reflections, which can alter the image.[16] Today, high quality digital cameras using infrared light to isolate the iris are used. The iris is then divided into vectors using a 2D Gabor wavelet that filters and maps the segments of the iris. The information that is recorded includes orientation and spatial frequency and the position of these areas.[17] Once this data is collected, an IrisCode is used to describe the patterns detected and two IrisCodes are compared in order to verify an individual's identity. The difference between the codes is labeled "Hamming Distance," which measures the dissimilarity between two irises. When two different irises are compared, they are statistically guaranteed to pass the test of statistical independence. However, iris recognition is based upon the failure of this test. "Failure" occurs when less than one third of the bytes in the codes differ. When images of the same iris are compared, they fail the test. Hence, a score of zero would indicate a perfect match. Glasses, contacts, and many new forms of eye surgery do not interfere with the ability to capture an accurate image of the iris. Nor are the blind excluded from iris recognition.

Retinal scanning identifies an individual based upon the pattern of blood vessels on their retina. Like iris recognition, a high quality digital camera must be used to capture the images. However, there is some concern that the retina becomes altered with age. Despite this concern, retinal scanning is widely used to restrict access to high-security areas. These systems are used by the CIA, FBI, and NASA.[18] User acceptance will be the greatest hurdle government officials will face if they opt to implement these systems on a nationwide scale.

---

15. COMM. ON TECH., NAT'L SCI. AND TECH. COUNCIL, IRIS RECOGNITION, http://www.biometrics.gov/Docs/irisrec.pdf (last visited Jan. 31, 2007).

16. *Id.*

17. *Id.*

18. Iris and Retinal Identification, http://et.wcu.edu/aidc/BioWebPages/Biometrics_Eye.html (last visited Jan. 31, 2007).

II. WHY USE BIOMETRICS?

A. *Increased Globalization*

Most proponents of biometric modalities cite national security needs in defense of biometrics in light of the fact that illegal immigration and terrorism have become a significant concern.[19] Intertwined with these concerns are international travel and trade considerations. Biometric systems offer a unique solution by aiding government officials (and businesses) in determining who to include and who to exclude with speed, accuracy and convenience. Such systems allow society to draw the delicate balance between national security and international commerce. Moreover, when compared to a cavity search or police interrogation, the nationwide application of biometrics is appealing in that most methods are unintrusive (i.e. finger and hand scans) and do not stray far from the identity verification practices with which we have grown accustomed. In a world where obtaining false documents and identification is only a click away, biometrics offer a pricey, yet attractive, alternative— identification and verification with a higher degree of certainty than current practices.

What makes these systems so useful is their ability to conduct one-to-many matches in large databases. For example, high-end automated fingerprint identification systems (AFIS) are highly accurate, scanning ten fingers with flat or rolled impressing and boasting failure-to-match and false match rates close to zero, depending on the matching algorithm used. They simply add physical and/or behavioral characteristics to identity information. The US-VISIT system adopted by the Department of Homeland Security captures and stores data concerning those entering the country.[20] Fingers are scanned and a digital photograph is taken in order to verify individuals before allowing them into the country.[21] The same is true of modalities used for verification purposes; except, instead of tracking criminals, biometrics can allow or restrict anyone's access to sensitive areas, as needed.

B. *The Dangers of the Internet*

Biometric systems can also combat phishing and identity fraud, the fastest growing crime problem in the United States. By using physical

19. ACCENTURE, THE FUTURE OF IDENTITY: BIOMETRICS SOLUTIONS TO ENHANCE THE PERFORMANCE OF BUSINESSES AND GOVERNMENTS 2 (2005), http://www.accenture.com/NR/rdonlyres/3919AF1E-2414-4E73-92AB-74FC1911281E/0/future_identity.pdf.

20. Ed Frauenheim, *Accenture Lands Homeland Security Deal*, June 1, 2004, http://news.com.com/Accenture+lands+Homeland+Security+deal/2100-1029_3-5223851.html.

21. *Id.*

identifiers, individuals do not need to deal with the expense and time-consuming nature of clearing their name if their identity is stolen. Rather than memorizing several different passwords, with a scan of one's finger, access to bank accounts and other private data can be achieved.[22] Recognizing the commercial benefit of this technology, stores such as CompUSA are selling mice with finger scanning technology to restrict access to one's computer files. Yet, what will likely become more common are methods such as the one adopted by the Albertson's grocery store chain. The store allows customers to register their fingerprints and bank accounts with a third party service such as BioPay or Pay By Touch and permits them simply to scan their finger rather than using a credit card.[23] Similarly, some computer manufacturers sell laptops with a fingerprint scanning capability, allowing online shoppers to pay by scanning their finger, rather than inputting credit card information.[24]

III. THE RISKS OF BIOMETRICS

Biometric modalities present legal questions that cannot be left for future generations to resolve. Since these systems are becoming more prevalent in numerous sectors throughout American society, the problems and challenges faced by personal identification and verification using physical characteristics must be addressed today. The central question is how government and law enforcement officials can adapt these techniques to protect an individual's privacy while achieving legitimate objectives.

If fingerprinting and drug testing are considered "searches" under the Fourth Amendment, one must ask if taking one's biological data through a biometric modality also constitutes a search.[25] It is clear from the U.S. Supreme Court's decision in *Katz v. United States* that the Fourth Amendment protects people rather than places.[26] In *Katz*, the Court held that Katz's expectation of privacy in a phone booth was

22. ACCENTURE, THE FUTURE OF IDENTITY: BIOMETRICS SOLUTIONS TO ENHANCE THE PERFORMANCE OF BUSINESSES AND GOVERNMENTS, (2005), http://www.accenture.com/NR/rdonlyres/3919AF1E-2414-4E73-92AB-74FC1911281E/0/future_identity.pdf.

23. Grace Wong, *Cash or plastic? How about fingerprint?*, July 20, 2005, http://money.cnn.com/2005/07/19/pf/security_biometrics/ (last visited Jan. 31, 2007).

24. *Id.*

25. KENNETH P. NUGER, NAT'L BIOMETRIC TEST CTR., SAN JOSE STATE UNIV., BIOMETRIC APPLICATIONS: LEGAL AND SOCIETAL CONSIDERATIONS, http://www.engr.sjsu.edu/biometrics/publications_consideration.html (last visited Jan. 31, 2007)

26. 389 U.S. 347 (1967).

unreasonable.[27] Notwithstanding the Court's decision, while reasonable minds could differ regarding the reasonableness of one's expectation of privacy when engaging in a telephone conversation in a closed telephone booth, when considering the characteristics of an individual's hand or iris, the answer seems much more straightforward. Few would argue that an individual's subjective expectation of privacy in their fingerprints, iris, and retina is not socially recognized as reasonable.[28] Accordingly, a Fourth Amendment challenge to the use of biometrics would likely be upheld.

A. *Technological Advances and the Shrinking Right to Privacy*

However, this perfunctory answer is somewhat unsatisfying, and for good reason. Changing social expectations of privacy influence Fourth Amendment rights.[29] As Steven Goldberg notes, the realm of privacy shrinks as technology develops.[30] Had thermal imaging devices been more prevalent at the time of the *Kyllo* decision, the Supreme Court would likely have reached a different result.[31] We now live in a society where biometric systems are used to pay for groceries, check out library books, gain entrance to private gyms, and speed through airport security. Such issues warrant the conclusion that biometric technology is in the "general public use."[32] This technology can hardly be labeled crude or primitive and has slowly become a part of everyday life for a segment of the general population. If we accept this as true, how can we reconcile limited Fourth Amendment protections with an individual's reasonable expectation of privacy?

B. *Biometrics As Applied to* Terry *Stops*

Of critical importance is the context in which biometric modalities are used. At the outset, it is important to recognize that the United States government is focusing its attention on applying biometrics to border

27. In *Katz*, the defendant was suspected of transmitting wagering information and the police recorded his end of the conversations by attaching a listening device to a phone booth without obtaining a warrant.

28. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

29. Kyllo v. United States, 533 U.S. 27 (2001).

30. Steven Goldberg, *Enhancing The Senses: How Technological Advances Shape Our View of the Law*, 109 W. VA. L. REV. 1 (2006).

31. Kyllo was suspected of growing marijuana in his home. Federal agents used thermal imagers to scan the roof and side of his apartment building. The U.S. Supreme Court held that obtaining information regarding the interior of the home by sense-enhancing technology that could not otherwise have been obtained without physical intrusion into a constitutionally protected area constitutes a search where the technology in question isn't in the general public use. *Kyllo*, 533 U.S. at 27.

32. *Kyllo*, 533 U.S. at 40.

security to identify and reject known (and suspected) terrorists and other individuals viewed as a "threat" to national security. Consequently, challenges to the use of biometric technology will likely occur in the criminal context and this Note focuses on biometric technology in this setting. Since this technology can only be used for identification and verification purposes, the questions this Note raises will most often apply where police officers briefly detain individuals for investigation. The question then becomes, how can courts balance the needs of law enforcement officials against the individual's right to privacy in a criminal setting? *State v. Flynn*[33] provides an example of when biometrics would most likely give rise to Fourth Amendment concerns. There, two suspects were stopped for investigation of a recent burglary and one refused to identify himself, although he admitted to carrying identification in his wallet. The officer removed his wallet and radioed in the suspect's name and was told that the suspect was wanted for an earlier crime. The court held that preventing an officer from ascertaining a suspect's identity would render a stop useless and noted that the search was a limited one that the suspect could have avoided by providing his identification. A biometric system would replace the use of a radio in this example with the same or a lesser degree of intrusiveness.

However, other courts have reached the opposite conclusion. In *People v. Williams*, a Michigan court ruled the act of looking through the suspect's wallet a violation of the Fourth Amendment, despite the officer's belief that the suspect was lying when he stated that he had no identification.[34] Although both *Flynn*, a *Wisconsin* case, and *Williams*, a Michigan case, involved lawful stops, opposite conclusions were reached. With biometric systems, it is likely that most of the resulting detentions would be characterized as lawful stops due to the fact that only those individuals who are a match in the system would be detained (i.e. those with a criminal history). Currently, IAFIS, the database used by the FBI, only contains the fingerprints of individuals with a corresponding criminal history. Similarly, suspected terrorists and other individuals with restricted access to high-security areas could be detained because their hand or eye scan yields a "hit" in a criminal history (or suspected terrorist) database linked to a biometric database and further investigation is needed. *Hiibel v. Sixth Judicial District Court* provides another useful example. There, the U.S. Supreme Court used *Terry* balancing to hold that the request for identity has an immediate

33. State v. Flynn, 285 N.W.2d 710 (Wis. 1979).
34. People v. Williams, 234 N.W.2d 541 (Mich. App. 1975).

relation to the purpose, rationale, and practical demands of a *Terry* stop.[35] The Court further held that the threat of criminal sanction helps ensure that the request for identity does not become a legal nullity; and that such threat does not alter the nature of the stop itself provided that the request for identification was reasonably related in scope to the circumstances which justified the stop.[36]

These cases are all instructive but precious few involve technology similar to that used in biometric modalities. Perhaps most informative is *United States v. Dionisio*, where a group of witnesses were subpoenaed to appear before a grand jury and provide voice prints. There, the Court held that the Fourth Amendment was not violated and that no preliminary showing of probable cause or reasonableness was required in such a case. What is relevant is the Court's discussion of the voice print requirement:

> the requirement that the witness give exemplars does not infringe upon Fourth Amendment rights, as 'the physical characteristics of a person's voice, its tone and manner, as opposed to the content of a specific conversation, are constantly exposed to the public,' so that 'no person can have a reasonable expectation that others will not know the sound of his voice.[37]

The Court's rationale does not support the conclusion that one's expectation of privacy in their physical and behavioral characteristics must always be upheld. In theory, one's fingerprints, eyes, and handprints are always on display. Moreover, even if individuals are more cautious with regard to consenting to fingerprinting, the law offers little protection when certain conditions are present. In *Hayes v. Florida*,[38] fingerprinting was deemed permissible if three requirements are satisfied: there is reasonable suspicion that the suspect has committed a criminal act; a reasonable basis for believing that fingerprinting would establish or negate the suspect's connection with that crime; and the procedure is carried out with dispatch.[39] But in *Davis v. Mississippi*, the Court cautioned that detentions for the sole purpose of obtaining fingerprints are

35. A *Terry* stop occurs when a police officer detains an individual on reasonable suspicion that they have or about to commit a crime. It is not considered an arrest. The officer may temporarily detain the person to request identification and question them regarding the suspected criminal activity.

36. Hiibel v. Sixth Judicial District Court, 542 U.S. 177 (2004).

37. 410 U.S. 1 (1973).

38. Hayes v. Florida, 470 U.S. 811 (1985).

39. *Id.*

no less subject to the constraints of the Fourth Amendment.[40] However, the Court noted that in narrowly defined circumstances, the fingerprinting process could be found to comply with the Fourth Amendment even though there is no probable cause in the traditional sense. The Court concluded that fingerprinting is less intrusive, inherently more reliable in solving crime, and not susceptible to the same weaknesses as an improper lineup. How can the use of biometrics be limited when probable cause is not required?

C. *Adapting Biometric Systems to Meet Fourth Amendment Requirements*

Biometric modalities if properly tailored can satisfy the requirements of the Fourth Amendment even in the absence of probable cause. Probable cause exists where the facts and circumstances known to the officer are sufficient to warrant suspicion that a crime was committed and that the person being detained committed that offense.[41] However, where an arrest warrant is not required, probable cause is not necessary; instead, the search must simply be reasonable. From an objective point of view, a fingerprint or facial scan as compared to a cavity search or "frisk," biometric technology seems minimally invasive, at best. Some might even prefer to have a finger scanned if it can resolve questions of identity more efficiently. As more and more people begin to scan their fingers (or hand, iris, etc) to enter their local gym or pay for groceries, the more common these biometric systems become. Given the level of comfort the public is displaying with regard to this technology, public reaction warrants the conclusion that biometrics is becoming a commonplace part of society where individuals are willing to relinquish their right to privacy in their fingerprints, irises, etc. and place them in the public domain. Although individuals currently cannot purchase biometric systems to restrict access to their homes, cars or other secured areas, if the fingerprint flash drives and fingerprint readers sold at CompUSA are any indication, application of biometric modalities to home security is on the horizon. Realistically, a court faced with this issue will need to distinguish between the various forms of biometric modalities and articulate which (if any) are so intrusive that their use violates the Fourth Amendment, just as courts have distinguished between drug tests, blood tests, fingerprinting and nonconsensual stomach pumping.

---

40. Davis v. Mississippi, 394 U.S. 721 (1969) (petitioner and 24 other youths were detained for questioning and fingerprinting in connection with a rape where only a general description was given and police had obtained a set of the assailant's fingerprints).

41. *See* Maryland v. Pringle, 124 S. Ct. 795 (2003).

For example, if one component of such a system includes a method identifying individuals according to their gait, the individual's subjective expectation of privacy would fail the second prong of Justice Harlan's two-part test.[42] In such a case a court's inquiry into the constitutionality of biometric identification and verification systems would allow the court to establish some guidelines. Outside of their home, the way in which an individual walks is typically exposed to the "'plain view' of outsiders" without manifestation of an intent "to keep [it private]." The very act of being outside contradicts assertions that the individual retains an expectation of privacy and a less stringent standard would be required. An analogy could be drawn to *U.S. v. Knotts*, where the Supreme Court held that there is a diminished expectation of privacy in an automobile because a car that travels on public roads and highways is open to public scrutiny.[43] The defendants did not have a legitimate expectation of privacy regarding information observable to the public such as movements of a car on public property. Yet, the implication is that anyone who walks outside automatically gives up their right to privacy in their gait. Logic, however, tells us that the way one walks is drastically different from the pattern of blood vessels in one's retina and it is difficult to extrapolate the *Dionisio* holding (the requirement that witnesses appear before a grand jury and provide voice prints did not violate the Fourth Amendment and no preliminary showing of probable cause or reasonableness was required in such a case) to a retina or iris, which seems inherently private.

A court faced with this issue would need to articulate a rule regarding the weight one's expectation of privacy (based upon the type of physical data involved) should be given. If a sliding scale is used, gait, as compared with an iris, retinal scan or facial scan (where a court would likely want to keep the right to privacy intact) would fall on the lower end of the spectrum. In light of the fact that multi-modal biometric systems will slowly become more prevalent, it will be imperative for courts to determine which types of biometric identifiers give rise to an expectation of privacy consistent with the *Katz* test,[44] i.e. how "invasive" the biometric modality is characterized. The issue of invasiveness would likely be a two-part inquiry taking into consideration what is done to the suspect's body and how law enforcement officials use the information. Courts can use this as the foundation from which they can assess the

42. In *Katz*, Justice Harlan announced a two-part test to be used when assessing an individual's Fourth Amendment claim. Under the test, a person must have exhibited an actual (subjective) expectation of privacy and the expectation must be one that society is prepared to recognize as "reasonable."

43. United States v. Knotts, 460 U.S. 276, 281–282 (1983).

44. Katz v. United States, 389 U.S. 347 (1967).

public's access to that specific type of technology and begin to develop standards relevant to biometric technology. Yet, the terrorism context raises a completely different set of problems.

The rationales articulated above do not extend to an environment plagued by a fear of terrorist acts against the United States. In this setting, biometrics systems are being used to identify someone who may or may not commit an act of terrorism once they are on U.S. soil. *Williams* and *Hayes* contemplate circumstances where detainees are stopped on reasonable suspicion of involvement in a crime. However, suspected terrorists will be detained on reasonable suspicion that they *might* commit a *future* crime (unless an outstanding warrant or some other intervening circumstance requiring arrest is present).[45] Given that national security is deemed an area best left to the executive branch, police officers and federal agents will be given more deference when dealing with suspected or known terrorists. This is the type of setting where law enforcement officials could use more intrusive scans as a means of identification and where we would encourage the use of multi-modal systems to heighten accuracy. Given that federal agencies typically compare the data they receive when an individual attempts to enter the country with data collected by other domestic and international organizations before allowing the individual to enter U.S. territory, implementing multi-modal systems could have the same effect, assuming that the necessary databases besides the AFIS/IAFIS system contain criminal history information. Taking the multi-layered screening approach and the ongoing "War on Terror" into consideration, courts are unlikely to second-guess determinations regarding who is allowed entry into the country and who is denied, in light of the fact that allowing the "wrong" person entry could have deadly consequences. While detaining suspected terrorists and other criminals from entering the United States is an important goal, the problems biometric data poses will not be as difficult to resolve in this

45. See US-VISIT Stops Murderers, Pedophiles and Immigration Violators From Entering The United States Through Biometrics and International Cooperation, http://www.findbiometrics.com/article/67 (last visited Feb. 16, 2007) (a Swiss national suspected of being a pedophile was sent back to France after a fingerprint scan indicated that he was wanted by Interpol). US-VISIT is a system developed by the Department of Homeland Security designed to verify an individual's identify when they attempt to enter the United States in an effort to facilitate travel while preserving national security. The process typically begins overseas, at the U.S. consular offices issuing visas, where visitors' biometrics (digital fingerscans and photographs) are collected and checked against a database of known criminals and suspected terrorists. When the visitor arrives at the port of entry, the same biometrics are used to verify that the person at the port is the same individual who received the visa. The US-VISIT system is currently being tested at many airports and seaports nationwide.

setting because law enforcement officials are given more latitude where national security is at stake.[46]

IV. CABINING BIOMETRICS

The best way for states to establish limits on the use of biometrics is to legislate or amend their state constitution to provide protections greater than those encompassed in the Fourth Amendment. States can set guidelines clarifying when and under what conditions biometric modalities can be used. Moreover, states should require that multi-modal systems be used to decrease the number of false identifications and false non-matches. Further, states can legislate so that law enforcement officials are prohibited from using biometrics systems as their primary means of identifying and verifying individuals. As Paul Rosenzweig suggests, biometric systems could be limited to verification or "one-to-one" matching, where the accuracy is higher.[47] A warrant could be required for all fingerprint scans or scans deemed to be "intrusive," unless exigent circumstances exist. The definition of a search could be broadened to address the varying forms of biometric technology or the offenses for which a police officer can conduct a fingerprint scan could be narrowly defined.

If biometric modalities are to be used to identify criminals and terrorists, for example, the success of the system will depend upon the strength of the database that is used. In order for the technology to be used properly, a criminal must be identified as such in the biometric database or must be linked to a criminal history database.[48] While the FBI's IAFIS system is the most comprehensive database among law enforcement organizations, fingerprints alone do not guarantee accuracy. Part of

46. For example, where an individual who has detonated bombs throughout Europe, but has eluded capture is flagged by Interpol as a suspected terrorist, when that individual attempts to enter the United States, his finger, hand or face could be scanned and the image would then be cross-referenced with Interpol's and other criminal history databanks. Once the system recognizes that this individual has been detained as a suspected terrorist, Customs officials can deny his entry into the country. Given the individual's criminal history and assuming that the state of national security was such that entry into the United States was being restricted due to perceived terrorist threats, few courts would question this act. The rationale for this deference stems from the view that the Executive Branch is best placed to make decisions concerning national security, not the courts.

47. Paul Rosenzweig & Alane Kochems & Ari Schwartz, *Biometric Technologies: Security, Legal, and Policy Implications*, June 21, 2004, http://www.heritage.org/Research/HomelandDefense/lm12.cfm (last visited Feb. 16, 2007).

48. In order for the linkage theory to withstand criticism, the criminal history database must have used the same biometric scans that I have discussed so that when a hand or iris is scanned, the new template can be cross-referenced with an older one, taken at the time the individual was detained on suspicion of a crime.

the appeal of biometrics is that the different methods can be layered to create a multi-modal system. Advocates suggest that this multi-layered approach be used rather than a single-layer approach to enhance accuracy. In addition, if one method should fail, verification and/or identification can still occur using another layer of the biometric technology. For these systems to achieve full-scale implementation, other biometric databases will need to be developed and those who have been convicted of a crime will need to be flagged within the database. When one considers the fact that the database of retinal images is very small, it is unlikely that many of the individuals in the database are flagged as suspected criminals. However, it might not be long before those booked at police stations will have their hands and faces scanned. This process will take time and cabining biometric systems will be difficult until these systems are put to their best use.

CONCLUSION

Biometric systems are not meant to be treated as the ultimate security solution. Legislatures must assess the strengths and weaknesses of these systems before allowing their full-scale use, especially in light of the ramifications of a false match. Biometric modalities are best used as another tool in a layered approach to security that should not be demonized and cast aside without further exploration. The key is to ensure that the government's infringement on privacy rights corresponds with its interaction with the individual and that it has the technological tools in place to achieve this goal. Biometrics differ from beepers, GPS, RFID chips, and other tracking devices. Whereas these devices allow the government to follow you wherever you go, biometric technology replaces "you" with a mere algorithm. Rather than watch your every move, law enforcement officials are unable to determine who "you" are until you are stopped by a police officer or attempt to access a restricted area.

One cannot avoid technology. Rather than escape it, time must be spent creating rules and guidelines for how this technology can be used to achieve legitimate governmental objectives without eradicating the protections the Fourth Amendment provides. State laws can guide courts if legislatures opt to address recent technological advances. The Supreme Court's ruling in *Kyllo* can be used as a baseline until biometric systems become a part of our every day lives. If the San Jose Mineta International Airport, Heathrow Airport and the Florida School District are any indication, we won't be waiting long.