SYRACUSE SCIENCE & TECHNOLOGY
LAW REPORTER

VOLUME 22 SPRING 2010 ARTICLE 2, PAGE 38

Biometrics, Retinal Scanning, and the Right to Privacy in the 21st Century

Stephen Hoffman*

INTRODUCTION

Imagine it is the year 2030. As you walk down your street to visit your favorite coffee shop, a camera mounted at the nearest intersection tracks your movements. Initially, you are just a set of pixels transmitted to a video screen somewhere; however, after your movement has been picked up by the camera, it uses algorithms based on general body and skull structure to pinpoint the location of your eyes. Once the camera has found your eyes, it projects an infrared beam of light into your eyes which would not be noticed because infrared light is not visible to the human eye. Using the reflection of the light from your retinas and choroids, the camera photographs the vasculature structure of your eyes and runs it against a database of known criminals, immigrants, and even people dissenting from popular opinion. If your retinal pattern matches that of a person listed in the database, the computer transmits this information to the proper authorities. All of this happens before you even step through the door of the coffee shop. This Orwellian[1] future of an omnipotent Big Brother is not consistent with a free democracy subservient to the people.

However, this is not the only worrisome issue presented by this scenario—what if private companies, instead of the government, are the ones running those cameras? What if a health

* J.D. Candidate 2010, University of Minnesota. The author would like to thank Professor Stephen Cribari for his help and suggestions on this work. Any substantive mistakes are my own.

[1] GEORGE ORWELL, 1984 (1949).

insurance company installs these cameras outside its offices to identify individuals and detect disorders and illnesses before they walk through the door? Retinal vascular patterns have been shown to anticipate future illnesses as well as conclusively identify several illnesses that the individual suffers from, and many of these are hereditary or genetic conditions. If the insurance company knows what you are susceptible to before you are personally aware, and uses this to refuse coverage or charge a higher premium for the policy you apply for, then it has appropriated something extremely private of yours without consent and may use this knowledge to profit from your supposed "condition," regardless of whether those future or current illnesses have manifested or will manifest themselves. Why should such an intrusive procedure be allowed without any concern for the privacy rights of those being examined?

I. BIOMETRICAL ANALYSIS AND ITS BACKGROUND

Retinal scanning, along with many other authentication techniques, falls under a branch of science known as biometrics. Biometrics or, more specifically, "biometric authentication" for purposes of this paper, is defined as the use of technology to automatically identify or verify the identity of people by physical or behavioral characteristics.[2] This idea of "automatic" identification is derived from the fact that, unlike most computer identification procedures such as entering a password or swiping a smart card, biometric identifiers use methods that require no additional knowledge but are still extremely difficult to counterfeit.[3] Some examples of biometric identifiers include fingerprints, facial structure, handwriting, and—which will be

[2] *See* JAMES WAYMAN ET AL., BIOMETRIC SYSTEMS 2 (2005); Lauren D. Adkins, *Biometrics: Weighing Convenience and National Security Against Your Privacy*, 13 MICH. TELECOMM. & TECH. L. REV. 541, 542 (2007).

[3] ROBERT HILL, RETINA IDENTIFICATION 1, *available at* http://www.cse.msu.edu/~cse891/Sect601/textbook/6.pdf.

discussed here—retinal structure.[4]

Biometric identification systems are grouped into two major categories: positive and negative identification.[5] Positive identification systems are used to test the hypothesis that the submitted image does belong to an individual enrolled in the system.[6] Positive identification systems are typically used in connection with high-security access or secure areas or networks. Such a system confirms that the individual is entitled to have access and is extremely useful in preventing multiple users from using a single enrolled identity. Negative identification systems, on the other hand, come into play when it is hypothesized that the submitted image does not belong to *any* individual in the system.[7] In essence, these systems are used to prevent a user from having multiple identities enrolled within the system.[8] This distinction between positive and negative identification systems is key in determining how the system will operate.

Biometric technologies fall into three general categories: high biometrics, lesser biometrics, or esoteric biometrics.[9] High biometrics are biometric technologies with a high accuracy rate and current working systems in operation, and also are based on "features that are

---

[4] Retinal scanning or imaging is actually somewhat of a misnomer. The scanning procedure uses infrared light to illuminate the retina, but the retina is "essentially transparent" to infrared light due to its wavelength. HILL, *supra* note 3, at 2. The reflection of the infrared light—which is used for the identification—is actually created by the collection of blood vessels in the choroid, which is just behind the retina. *Id.* at 2-3.

[5] WAYMAN, *supra* note 2, at 5.

[6] *Id.*

[7] *Id.*

[8] *Id.*

[9] John D. Woodward, *Biometric Scanning, Law & Policy: Identifying the Concerns–Drafting the Biometric Blueprint*, 59 U. PITT. L. REV. 97, 102 (1997).

considered truly consistent and unique."[10] These consist of fingerprint, retinal, and iris imaging.[11] Lesser biometrics, on the other hand, have reasonable accuracy and systems in operation but are not based on truly unique characteristics.[12] These characteristics include hand geometry, facial structure, and voice structure.[13] The term "esoteric biometrics" is used to describe experimental techniques or those in development.[14] Some examples of esoteric biometrics are vein measurement and the chemical composition of body odor.[15]

A. Theory and Advantages of Retinal Scanning

1. Introduction to Retinal Scanning Theory and the Scientific Method

Retinal scanning is widely accepted in the scientific community as being a valid method for authentication of people. This acceptance is based, as other reputable biometric systems are, on successful testing and hypothesizing using the scientific method.[16] Other systems and techniques which do not successfully utilize the scientific method yet are touted as accurate or true comprise a category known as "junk science."[17] Under the *Frye* standard,[18] which allowed

---

[10] John D. Woodward, *Biometric Scanning, Law & Policy: Identifying the Concerns–Drafting the Biometric Blueprint*, 59 U. PITT. L. REV. 97, 102 (1997).

[11] *Id.* at 102-03.

[12] *Id.* at 105.

[13] *Id.* at 105-07.

[14] *Id.* at 108.

[15] John D. Woodward, *Biometric Scanning, Law & Policy: Identifying the Concerns–Drafting the Biometric Blueprint*, 59 U. PITT. L. REV. 97, 108-09 (1997).

[16] CHRISTINE BECK LISSITZYN, FORENSIC EVIDENCE IN COURT 114-15 (2008).

[17] *See id.* at 113.

forensic evidence to be presented as long as the underlying theory was "generally accepted," false scientific theories and hypotheses such as the curative properties of bloodletting could be brought into court, usually in what is called the "battle of the experts."[19] However, the codification of Article VII of the Federal Rules of Evidence in 1975,[20] as well as the Supreme Court's determination that Article VII legislatively overruled *Frye*,[21] brought in a new standard for presenting scientific theories by experts. Under this new standard, delineated in *Daubert v. Merrell Dow Pharmaceuticals*,[22] expert testimony given regarding forensic science and biometrics is generally acceptable when it provides reliability and accuracy.[23] Because of this, a biometric measurement can almost exclusively be brought into court only if it possesses most or all of the five factors of an ideal biometric identifier.[24]

---

[18] Frye v. United States, 293 F. 1013 (D.C. Cir. 1923).

[19] LISSITZYN, *supra* note 16, at 114. This "battle of the experts" still takes place today under the heightened standard announced in *Daubert*, but experts must present scientific evidence regarding the accuracy and reliability of the theory or method underlying the offered evidence. Daubert v. Merrell Dow Pharm., 509 U.S. 579, 589-91 (1993).

[20] FED. R. EVID. art. VII.

[21] *See generally Daubert*, 509 U.S. 579 (1993).

[22] *Id.*

[23] LISSITZYN, *supra* note 16, at 93. The *Frye* standard is still used by many courts and is even used as one prong of the *Daubert* test. *Id.*

[24] WAYMAN, *supra* note 2, at 3.

2. The Five Characteristics of the Ideal Biometric Identifier[25]

a. Distinctiveness

Retinal scanning, as mentioned above, is considered to be extremely accurate and based on the analysis of a truly unique, or distinctive, characteristic.[26] This biometric is determined by the blood vessel patterns in the human eye, which was first discovered to be unique in 1935.[27] A study performed in the 1950s examined similar characteristics between identical twins and found that, of all the factors compared, "retinal vascular patterns showed the least similarity."[28]

b. Robustness

However, uniqueness is not the sole criterion for whether a particular biometric analysis is useful for identification or authentication purposes—uniqueness is unimportant if the thing being measured is not consistent or stable, otherwise termed "robustness" in biometrics.[29] For example, fingerprints are very stable and consistent since they do not change over the course of one's life.[30] Retinal vascular patterns are similarly very stable and consistent and therefore make retinal imaging a strong biometrical method.[31]

---

[25] WAYMAN, *supra* note 2, at 3. The ideal biometric measure is distinct, robust, available, accessible, and accepted. *Id.*

[26] *See supra* notes 10-11 and accompanying text.

[27] HILL, *supra* note 3, at 2.

[28] *Id.*

[29] WAYMAN, *supra* note 2, at 542.

[30] Federal Bureau of Investigation, *Fingerprint Identification* 1, *available at* http://www.fbi.gov/hq/cjisd/ident.pdf.

[31] Robert Hill, the inventor of the first retinal identification system, posits that of all the physical features unique to individuals, "none is more stable than the retinal vascular pattern." HILL,

c. Availability

In an attempt to find the ideal biometric, availability is the next quality to be considered.[32] In order for a characteristic to be "available," the entire population or at least a substantial proportion of it should have the measure in multiples.[33] For example, fingerprints and retinal vascular patterns would be available characteristics.

d. Accessibility

An accessible measure is one that is "easy to image using electronic sensors."[34] Fingerprinting is a prime example of an accessible method because the person being measured must simply place his hand onto a screen, at which point electronic sensors can measure them.

e. Acceptability

The final, yet important, characteristic of an ideal biometric system is that people accept (rather than reject) the measurement being taken.[35] This generally requires two considerations. First, whether people find the measurement to not be so intrusive as to make them too uncomfortable during the assessment. To illustrate this clearly, imagine that people would be required to disrobe and have their genitalia measured as an identification technique (assuming that scientific studies had conclusively shown that human genitals are unique and consistent

---

supra note 3, at 2. However, as will be discussed shortly, retinal vasculature is not completely invulnerable to change over the person's lifetime and many medical and physical conditions can change the structure and appearance of a person's retinal vascular pattern.

[32] WAYMAN, *supra* note 2, at 541.

[33] *Id.* at 542.

[34] *Id.*

[35] *Id.* at 546.

among individuals). Due to the physical and emotional intrusiveness of the measurement and other things such as cultural or religious beliefs inconsistent with such a technique, this measurement would be very unlikely to be widely accepted by the public. Second, whether people accept the underlying theory on which the measurement is based. For example, fingerprinting has been generally accepted as being an extremely useful method of identification for the last 100 years and so has been accepted under this second element.

3. Two Primary Characteristics and Their Statistical Significance

The first two qualities described above, robustness and distinctiveness, also provide scientists and analysts with an objective standard by which to judge the efficacy of the system. The robustness of the system is measured by the "false non-match rate," or the probability that the image submitted will not match an enrolled image.[36] Statistically speaking, this is known as Type I error and is important in determining the accuracy of the system to a particular level of statistical significance.[37] The system's distinctiveness, on the other hand, is measured by its "false match rate," which is the probability that the image submitted will match another user's enrolled image.[38] In contrast, this probability is termed Type II error and is instrumental in determining the reliability of the method across the population.[39] With such normalizing of the system, the quality of the biometric measurement or system can be determined population-wide.

[36] WAYMAN, *supra* note 2, at 546.

[37] *Id.*

[38] *Id.*

[39] *Id.*

B. Uses for Biometric Systems

Biometric authentication systems generally have one of two uses: to verify an individual's identity or to identify a user based on his biometric credentials.[40] Verification, on one hand, is when a person known to the system and already identified has her identity confirmed by the biometric analysis. This is known as a "one-to-one" mapping since the individual is only compared with her own information to confirm her identity.[41] On the other hand, identification takes place when a person believed to be in the system uses biometric readings in order to match the individual in the entire database of those enrolled in the system.[42] Identification provides what is termed a "one-to-many" mapping because the individual is compared to others enrolled in the system as opposed to only her.[43]

One primary difficulty in making retinal imaging more widespread is user discomfort with the systems. Current systems require users to position their eyes, which must be wide-open for the duration of the scan, less than an inch from the retinal scanner while focusing on a

---

[40] Darcie Sherman, *Biometric Technology: The Impact on Privacy*, Law Research Institute Research Paper Series CLPE Research Paper No. 5/2005 3 (2005), *available at* http://ssrn.com/abstract=830049.

[41] Retinal scanning is considered a verification technique where the individual's retinal vascular pattern is compared to his alleged identity in the system. However, with advances in technology and dramatic increases in computer processing speeds, this may not be the case in the future. If Moore's Law is correct in its hypothesis of exponential increases in computer processor speeds over time, retinal images could be compared between an individual and other people enrolled in the system similar to the way fingerprints currently are.

[42] *See* source cited *supra* note 40, at 2-3.

[43] An example of identification is shown by fingerprint analysis and matching. The person's fingerprint is compared to those of a large number of persons enrolled in the system or even all of the persons enrolled. *Id.* at 2.

target.[44] The scan generally takes from 10-15 seconds and, if an accurate reading was not made such as due to blinking or eye movement, may need to be performed more than once.[45] Because of the obtrusiveness of the scan, retinal scanning and its counterpart iris scanning are slow to gain widespread public acceptance.

Another difficulty is that the retinal vascular patterns can give information besides simply identification or authentication, which is a major difference compared to other biometric methods. An examination of these patterns by an expert can indicate whether the individual suffers from common illnesses such as diabetes, arteriosclerosis, or hypertension, or from more unique circumstances such as AIDS, high blood pressure, or even intravenous drug abuse.[46] Because of this, retinal imaging and other biometric technologies cannot be used in all situations. To illustrate this, imagine that a health insurance company requires an individual to undergo a retinal scan both while creating his policy and at any emergency room he visits in order to ensure that he is the one using the health insurance and not some impostor. If the health insurance company can use these retinal images to determine which of an assortment of maladies a person suffers from, it could use this information—which is supposed to be used only for identification or authentication—to charge higher rates, provide more limited coverage, or even refuse coverage completely.

In addition, although the retinal vascular structure is very stable, it is not impervious to change. Age-related macular degeneration and other forms of degenerative retina disorders

---

[44] HILL, *supra* note 3, at 11-12.

[45] *Id.*

[46] John D. Woodward, *Biometric Scanning, Law & Policy: Identifying the Concerns–Drafting the Biometric Blueprint*, 59 U. PITT. L. REV. 97, 115 (1997).

(including severe astigmatism) cause a large change in the pattern of the blood vessels used for biometrics.[47] Because of this, retinal scanning may not necessarily be reliable for verifying one's identity. This causes ideological problems in the context of the criminal justice system and convicted criminals. If a convicted criminal is released after having his retina scanned, he can "game" the system by simply bad genetics or improper eye care. If he is subsequently scanned again—say, on suspicion of committing another crime—his condition may allow him to avoid identification. Even if experts in retinal degeneration were called in to determine what, if any, medical conditions he could or did have through his retinal image, they could not view his later, altered retinal image and be able to deduce that it was the same man. Because of how complex and unpredictable the vascular patterns in the eye develop and the additional complexity and unpredictability of the alterations caused by retinal degeneration, it is impossible to know exactly how the vasculature will degenerate due to disease *X*. The human body is too variable on a population-wide scale and there are too many confounding factors that come into play to be able to predict exactly how the vascular pattern will change due to retinal degeneration.

Furthermore, expert review of retinal images can determine what medical conditions a person has and, if a genetic link is known or hypothesized to account for those conditions, indicate other conditions or disorders the person does or might suffer from.[48] Retinitis pigmentosa is an example of such a condition, with over 45 causative genes identified which

[47] For several illustrations from clinical studies of the different characteristics of ocular degeneration, *see* Eliot L. Berson, *Retinal Degenerations: Planning for the Future*, *in* RECENT ADVANCES IN RETINAL DEGENERATION 21-23 (Robert E. Anderson, Matthew M. LaVail & Joe G. Hollyfield eds., 2008).

[48] *Id.* at 23-24. "Over 100 genes have been implicated in human hereditary retinal degenerations." *Id.*

account for 50-60% of all cases.[49] As this suggests, if a retinal image suggests a person suffers from or is susceptible to this condition, there may be evidence that the individual suffers from or will suffer from other conditions which are caused by the same gene or genes. This is the case regardless of whether the person actually develops the feared conditions.

C. Retinal Scanning and Its Implications for the Right of Privacy

Although the uniqueness and consistence of retinal imaging and retinal vascular patterns support its use in identification and authentication, there are also equally plausible arguments against its use. For example, the fact that retinal vascular patterns are unique and consistent also shows one of its major flaws—compromise of a biometric system with this information would make it impossible to make that information secure. Unlike in traditional network security settings where users enter a password or swipe a smart card, such unique and personal information cannot be "reset" or changed to maintain the user's enrollment in the system. Therefore, a system based completely on retinal vascular patterns and no other biometric or alternative method of authentication or identification would be useless if an unauthorized person can access this information and help counterfeit the required credentials. Succinctly put, "[t]he theft of biometric information amounts to permanent identity theft."[50] Biometric analysis is useful if it measures an immutable and unique characteristic. However, if the characteristic being measured is truly immutable, the individual generally cannot and should not be required to

[49] *See* source cited *supra* note 47, at 23.

[50] Steven C. Bennett, *Privacy Implications of Biometrics*, 53 PRAC. LAW. 13, 17 (2007). Many scientists and biometric theorists strongly suggest using multimodal methods of biometric analysis. Therefore, rather than using only one biometric measure (e.g., retinal vascular pattern) as would be used in a unimodal system, multiple biometric measures would be taken to greatly reduce the opportunity or attractiveness of defrauding the system. *See generally* David Usher et al., *Ocular Biometrics: Simultaneous Capture and Analysis of the Retina and Iris*, *in* ADVANCES

alter or change his compromised characteristic in order to render his identity secure again.[51]

As discussed earlier in the health insurance hypothetical, another key issue is that of anonymity in biometrics. If such personal information as health conditions and illnesses, as well as statistical inferences regarding particular conditions (e.g., if African-Americans are more likely than members of any other ethnicity to suffer from diabetes, a random retinal scan of a diabetic individual may suggest that he is African-American) are illuminated by retinal scanning, then the scan is providing more information than simply that of verification or identification. However, the purpose of a biometric system is to verify or identify users of the system. If the system is used for more than that, it would not matter whether the individual is an enrolled user or an unaware party being subjected to the scan—the information could be collected from anyone and a centralized database or similar storage methods would be unnecessary. Because of this, the privacy implications of biometric analysis have to be considered in-depth.

Privacy, as Professor John D. Woodward, Jr. illustrates, generally falls under three categories: physical privacy, decisional privacy, and informational privacy.[52] Physical privacy is that which Justice Louis Brandeis described in his dissent in *Olmstead v. United States*—the "right to be let alone."[53] This is also known as the right to be free from contact by others or

---

IN BIOMETRICS 133 (Nalini K. Ratha & Venu Govindaraju eds., 2008).

[51] For example, if a person's fingerprint pattern is rendered unsecured because of unauthorized system access, the person, who has done nothing wrong or improper, should obviously not be forced to have his fingerprints chemically or surgically altered simply to maintain the integrity of the system.

[52] John D. Woodward, Jr., *The Law and the Use of Biometrics*, *in* HANDBOOK OF BIOMETRICS 357, 360-62 (Anil K. Jain et al. eds., 2008).

[53] Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

monitoring agents.[54] The Founding Fathers valued this form of privacy highly and because of this drafted the Constitution with those concerns in mind, such as by ratifying the Fourth Amendment to the Constitution.

Decisional privacy, the next of the three categories, is focused on the freedom of letting individuals make private choices regarding personal matters without government interference.[55] An example of this type of privacy is shown in *Planned Parenthood of Southeastern Pennsylvania v. Casey*,[56] regarding procreation and contraception.

The third category with the most serious implications for biometric technologies, such as retinal scanning, is information privacy. Information privacy is the freedom of the person to limit access to certain personal information about him. This becomes a very serious issue when biometric measures give personal information without any concern for the person being analyzed. In addition, this raises many ethical problems when the information discovered is life-changing. For example, if a person is determined, after an analysis of her retinal vascular pattern, to have contracted AIDS, is the analyst or supervising firm required to disclose this information to the individual? Many would say yes, but what if a retinal image is only allowed if used in the course of verification or identification of a user? Since verification and identification are focused specifically on providing anonymity (hence, one major reason for having biometric analysis performed by a computer system), this would defeat any appearance of anonymity and thus be used in ways that biometrics are, or ought to be, by definition, unallowable.

---

[54] *See* source cited *supra* note 52, at 361.

[55] *Id.*

[56] Planned Parenthood of Southeastern Pennsylvania v. Casey, 505 U.S. 833 (1992).

CONCLUSION

Biometric analysis is a very important and revolutionary method for identifying or verifying individuals. Although fingerprinting was the first generally accepted biometric that was tested, technology has come a long way in creating many other and more precise methods of analysis. Retinal scanning, otherwise known as retinal imaging or retinal vascular pattern analysis, is one of these recent technologies and provides many benefits over other biometric methods. However, there are several attendant issues that must also be considered. Particularly troubling are the privacy implications of retinal scanning when such a technique can be used to determine private information personal to the individual being scanned. Information such as current and prospective illnesses or conditions a person suffers from or will suffer from, as well as recognizing genetic links to other conditions, can be discovered simply by analyzing retinal vascular pattern. This must force a critical eye toward such a technique, which has its expressly given purpose to provide security while preserving anonymity.

In order to prevent an Orwellian future where "privacy" is merely a word found in the dictionary, there must be oversight to prevent Big Brother, or Big Business, from using this information to discriminate among members of the public. If we do not, the Thought Police shall no longer be restricted to fiction and freedom as we know it could be impaired beyond remedy.