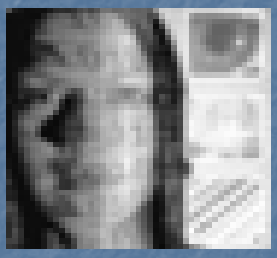
Biometrics Meets the Courts; Latent Prints and Other Methods of Identification Under Scrutiny



West Virginia University, Biometrics and The Law, March 27, 2006

Anjali R. Swienton, M.F.S, J.D.

The opinions, findings, and conclusions or recommendations in this presentation are those of the author and do not necessarily reflect the views of any associated agencies

Biometrics

- Automated methods of recognizing a person based on a physiological or behavioral characteristic.
- Among the features measured are face, fingerprints, hand geometry, handwriting, iris, retina, veins, and voice.
- How make a determination of a “match”?

The Biometric Consortium
http://www.biometrics.org/intro.htm

Biometrics Considerations

- Universality – everyone should have
- Uniqueness – no two people share
- Permanence – no variance over time
- Collectibility – easy and measurable
- Performance - accurate
- Acceptability – nonintrusive methods
- Circumvention – difficult to deceive

Advantages:

- Convenient and accurate
- Biometrics link events to a particular individual (vs. a token that can be stolen, misplaced, forgotten or forged or a password that can be forgotten, shared or observed)
- User friendly, low level of intrusiveness
- Ability to quickly scan large databases of information to produce results
- Useful for civil applications

Disadvantages:

- Newer biometrics may have high accuracy but need more research to establish uniqueness
- Especially important when used for criminal id

Differences between Biometrics and other Forensic Disciplines

- Toxicology
  - based on known and reproducible chemical composition of substances
  - When using confirmatory tests (e.g., GC Mass Spec) results are presented in absolutes “the substance tested IS cocaine”

Differences between Biometrics and other Forensic Disciplines

- DNA (based on principles of genetic inheritance)
  - Use statistical models and existing databases to produce estimated frequencies of a random match (high numbers, but not certainties)

Differences between Biometrics and other Forensic Disciplines

- Pattern matching evidence (firearms, toolmarks); Hairs/Fibers
  - Produce results of similarities based on class and individual characteristics
  - Degree of subjectivity involved

Differences between Biometrics and other Forensic Disciplines

- Biometrics
  - Use algorithms for comparative analysis
  - How determine the number of various possibilities for any given metric (polymorphism)?
  - Is some measure of quantitation needed to give the fact finder a frame of reference?
  - Depending on technique used, results are presented in a variety of ways

Science vs. Technical

- Methods grounded in science (DNA) vs. methods developed for, and used by, law enforcement (latent prints, ballistics)
- Even the Court recognized a difference (to a degree) with *Daubert* followed by *Kumho Tire* to close the gap

Latent Prints as a Model for Biometrics

- Numerous challenges
- To date, none have been granted
- The underlying question – does the current status of fingerprint examination research satisfy the legal admissibility standard? remains

Editorial in Science

"It's not that fingerprint analysis is unreliable. The problem, rather, is that its reliability is unverified either by statistical models of fingerprint variation or by consistent data on error rates."

Dr. Don Kennedy

Fingerprint Comparison

Based on assumptions of **uniqueness** and **permanence** of friction ridge patterns

- Underlying assumptions are not at issue
  - Judicial notice
  - Data from embryological development and statistical studies
- Comparison techniques used to make identifications are

Examiner's Fallacy

- Bait and switch - instead of addressing the critical issue of the accuracy of latent print source attribution, switch the focus to proving that all fingerprints are *permanent* and *unique*, issues that many courts have accepted
- Of note: uniqueness is unprovable whereas accuracy can be measured

Dr. Simon Cole

Lab vs. the courtroom

When techniques used in the lab are brought into the courtroom, must play by the rules of the court

For scientific or technical testimony, those rules include satisfying *Daubert* and reliability

Reliability and Validity

- Validity – ability of a test procedure to measure what it is supposed to measure (accuracy)
- Reliability – whether the same results are obtained each instance in which the test if performed (consistency)

Validity includes reliability but converse may not always be true

Accuracy implies a continuous measurement whereas validity seems to imply an either-or-judgment

The more accurate a specific technique is, the more valid it may be considered

So Where's the Problem?

- Absolute Identification - when match is called the examiner is claiming that the latent print necessarily came from the individual in question to the exclusion of all other fingers in the world.
- Once find a match, stop looking...
- "Zero error rate"
- No uniform standards for making comparisons and identifications
- Subjectivity aspect of identifications

Byron Mitchell case

- *United States v. Mitchell, Cr. No. 96-407*
- First *Daubert* challenge
- 1999 Philadelphia
- Defense motion denied

ACE-V

- **Analysis** – determine whether available ridge detail is sufficient, quantitatively and qualitatively, for individualization
- **Comparison** - Systematically compare various friction ridge arrangements and shapes including relative pore position where possible

ACE-V

- **Evaluation** - evaluate whether the concordance is of sufficient quantity and quality to permit a conclusion that they were made by the same portion of friction skin.
  - Final decision is subjective
- **Verification** - every individualization must be confirmed by another qualified examiner working independently

Daubert Factors

- Testing
- Error Rate
- Standards Controlling the Technique's Operation
- Peer Review
- General Acceptance

Plaza I

The question:
Are fingerprint identifications scientifically reliable under FRE 702 and *Daubert* factors?

All scientific testimony must be relevant and reliable...derived by the scientific method.

179 F. Supp.2d 492
January 7, 2002

Testing

Gov claims technique has been tested for 100 years by being admitted in court.

Pollack:

- this does not test the technique
- adversarial testing in court is not what the *Daubert* court meant
- scientific methodology today is based on generating hypotheses and testing them to see if they can be falsified

Testing

- In United States v. Sullivan the court found that "while the ACE-V methodology...appears to be amenable to testing, such testing has not yet been performed"
- (*United States v. Sullivan* 2003 at 704)

Research

Much research exists on fingerprints but none address the issue at hand

Instead, ongoing research seeks to clarify points not in contention such as:

- formation of friction ridge patterns in utero
- development techniques of latent prints
- search algorithms for automated systems (e.g., AFIS)

Error Rate

Gov divides error into methodology and practitioner error.

Claim methodology error is irrelevant and that practitioner error can be detected and corrected by another qualified examiner

If scientific method is followed, error in the analysis and comparative process will be zero

Error Rate

- If evidence is produced of a forensic match, "...a proper assessment of the probative value of that match requires awareness of the chance that a mistake was made..."
- Irrelevant whether the mistake was a method error or a practitioner error, affect is the same

Michael Saks, Jonathan Koehler, Science 8-05

Error Rate

"And we profess as fingerprint examiners that the rate of error is zero. And the reason we make that bold statement is because we know based on 100 years of research that everybody's fingerprint are unique, and in nature it is never going to repeat itself again"

(People v. Gomez 2002 at 270)

Error Rate – Casework Fallacy

- Claiming that 100 years of practice constitutes validation and proof of a zero error rate
- Casework, trial testimony about casework or millions of database searches are not “tests” of the accuracy of the technique because there is no guarantee that an inaccurate result would be detected

AFIS

- Citing billions of comparisons AFIS conducted as proof of validation of the technique
- AFIS does not declare matches or conclusions of any kind, it simply produces a list of possible candidates which can be manipulated by the analyst when setting up the search criteria

FBI Survey in Mitchell Case

Prints sent to 53 labs

34 responded

8 failed to make identification.

Sent enlarged prints back for re-examination.

All labs successfully identified prints.

Reasons given for labs' failure to make original identifications

- Examiner didn't know survey was related to a *Daubert* hearing
- Photos of 10-print cards or latent prints were insufficiently clear
- 3 of the examiners just screwed up
- Inexperience
- Insufficient time
- Examiner attitude toward the survey was not as serious as it should have been
- It was late in the day and examiner was probably tired

Error Rate

Pollack:

Can't have a fingerprint examination without an examiner. People make errors, therefore, there has to be an error rate associated with the process. The rate of those errors has to be an important part of evaluating whether or not the process works

Error Rates

- Best way to determine the frequency with which errors occur is to conduct blind external proficiency tests using realistic (evidence-like) samples
- Only way to know IF an error has occurred is when someone already knows the "correct" answer

Validation Study

- Measure of accuracy of techniques (used for making source attributions, NOT of uniqueness of all fingerprints)
- Outcome would be an accuracy rate, range or curve not an absolute

Proficiency vs. Validity

- Proficiency test tests the analyst's ability
- Validity study tests a particular scientific technique
- Even if analyst is using a "valid" technique, he/she could still make a performance error

Standards Controlling the Techniques

- History of different number of Galton point requirements country to country
- No mandatory qualification standards for individuals to become fingerprint examiners, no uniform certification process
- *With such a high degree of subjectivity (in making final identity decisions) – difficult to see how fingerprint identification is controlled by any clearly discernible set of standards to which most examiners subscribe*

Peer Review

Courts have claimed that the verification phase of ACE-V process constitutes peer review

Peer Review

Pollack:

- *numerous writings exist that discuss fingerprint identification techniques but it is not apparent that their publication constitutes submission to the scrutiny of the scientific community in the Daubert sense*
- when identification decisions are made subjectively, another subjective opinion rendered in concordance by another examiner does not make the initial conclusion scientific, or constitute peer review

General Acceptance

Gov claims that because fingerprints have been admitted in court for over 100 years they have been accepted

General Acceptance

Pollack:

- general acceptance by fingerprint examiner community does not meet the standard set by FRE 702. Fingerprint examiners do not constitute a scientific community in the *Daubert* sense
- general acceptance does not help show that an expert's testimony is reliable where the discipline itself lacks reliability
- fingerprint examinations are generally accepted among fingerprint examiners but that in itself is not enough

The Ruling

Up to the evaluation stage, a fingerprint examiner's testimony is descriptive, not judgmental. Allow testimony of how prints were obtained and any similarities observed, but no testimony to ultimate conclusions of identity

Plaza II

Government filed motion to re-hear the case, Pollack agreed. This time he came to the conclusion that although the technique still failed on testing, the other factors (error rate, peer Review and publication and general acceptance) were met by finding that fingerprint identification was not a science

188 F.Supp.2d 549
March 13, 2002

Testing

Still not met (though Pollack addresses this in his ruling)

Error Rate

FBI proficiency tests scored high from 1995 to date.

Proficiency tests are less demanding than desirable, but defense offered no proof that certified FBI examiners as a group have not achieved at least an acceptable level of competence

Error Rate

In the absence of actual data on rate of error, since FBI examiners rarely make mistakes on proficiency tests, it stands to reason that they rarely make mistakes when presenting ACE-V testimony in court

Standards

Pollack:
Standards prescribed for qualification as an FBI examiner are clear

However, the *Daubert* criteria for standards refer to standards for the **techniques** themselves, not the examiner. This is not addressed in the opinion at all

Peer Review

Fingerprint examiners are not scientists so forensic journals in which their writings on fingerprint identifications appear are not scientific in the *Daubert* sense. This should not go against the utility of their work

General Acceptance

General acceptance should not be discounted because examiners have technical knowledge and are thus not members of the scientific community (he had already deemed general acceptance satisfied in Plaza I)

Subjectivity

Pollack disagreed with himself, stating there are many situations in which an expert's manifestly subjective opinion is regarded as admissible evidence in an American courtroom

Ruling I vs. II

	I	II
Testing	N	N
Peer Review	N	Y
Error Rate	N	Y
Standards	N	Y
General Accept	Y	Y
Admit Testimony	N	Y

What changed his mind?

- First case was decided based only the record
- During the appeal he heard witnesses from the FBI testify in person
- What did they say the second time around that was not already in the record from round 1?

The Ruling

- *Contrary to my opinion in my January 7 opinion, I am now persuaded that the standards which control the opining of a competent fingerprint examiner are sufficiently widely agreed upon to satisfy Daubert's requirements*
- *Scientific tests of ACE-V would clearly aid in measuring ACE-V's reliability, but as of today, no such tests are in hand. For NIJ or other institutions …to sponsor such research would be all to the good. But to postpone present in-court utilization of this "bedrock forensic identifier" pending such research would be to make the best the enemy of the good*

Current public interests like security and justice demand that only the best and most reliable science be proffered in court. Pollack's suggestion is a good first step, but the reality is, that until courts **demand** proof, examiners have no incentive to do the research.

No way to know how many wrongfully incarcerated there may be who are there, at least in part, due to fingerprint examinations

Cowans

- Stephan Cowans – officer shooting in Boston 1997.
- Cowans was convicted on eyewitness evidence and a left thumb print with a 16 point match confirmed by 2 BPD examiners and 2 defense experts.
- DNA testing performed on several evidence items later exonerated him
- The fingerprint was reexamined and found not to match him

Science vs. Law

- Science is an ongoing collaborative process
- Law seeks final resolution through the adversarial system
- Science seeks truth
- Law seeks justice
- Both will be served by conducting research on the ACE-V technique

Science for Science's Sake

- Science teaches that you can't know the answers until you ask the questions.
- Science is a process or method by which factual statements or predictions are devised, tested, evaluated, revised, replaced, rejected or accepted.
- In light of a concrete case where we know something went wrong (Cowans), we must look into the what, why and how

Who should be responsible for conducting the research?

- The greater the stakes in property, lives and liberty, the more incentive the system should have to ensure that only proven reliable methods are being testified to in court.
- Responsibility as scientists who testify in court to provide it.
- Responsibility of judges who admit the testimony to demand it.

Daubert and FRE 702 provide guidance for admissibility of expert evidence

Courts can continue to say that fingerprint analysis is reliable, but that alone does not make it so. Only scientific testing will provide the empirical data to prove it.

Other Biometrics

- May endure the same types of challenges as latent prints without the advantage of 100 years of acceptance
- Specific expertise required to employ many of the techniques
- Some level of subjectivity still involved
- Even products for "commercial" use may end up in court

Other Biometrics

- Public may be suspicious of “new fangled technology”
- CSI Effect
- Reality/limitations of technology vs. reality

Retinal scans

- Uses a low-intensity light source and a delicate sensor to scan the pattern of blood vessels at the back of the retina
- Unique to each individual

Retinal scans

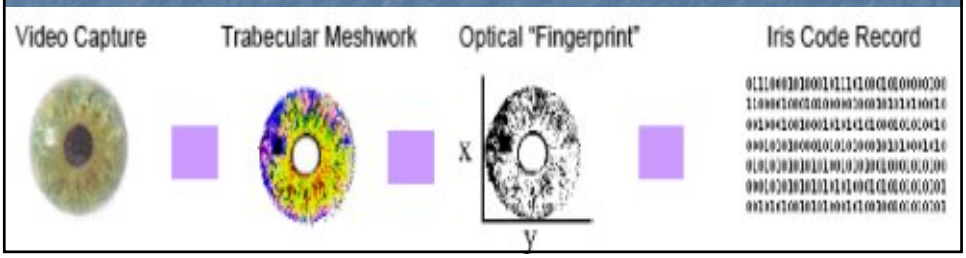
- Difficult to fake because no technology exists that allows the forgery of a human retina
- Retina of a deceased person decays too fast to be used to fraudulently bypass a retinal scan
- Published error rate of 1 in 10,000,000
- Can be affected by diseases such as glaucoma, diabetes, high blood pressure, etc
- What databases are used?

Iris Recognition

- Combines computer vision, pattern recognition, stats, and optics
- Fast and accurate recognition of id based on digital image of the scanned eye
- 266 unique spots
- Works with glasses and contact lenses

Iris Recognition

- B&W high resolution image, analyzed, processed into optical fingerprint, translated into digital form, uploaded and searched vs. database
- 1 second to capture image, 100,000 IrisCodes per second search capability

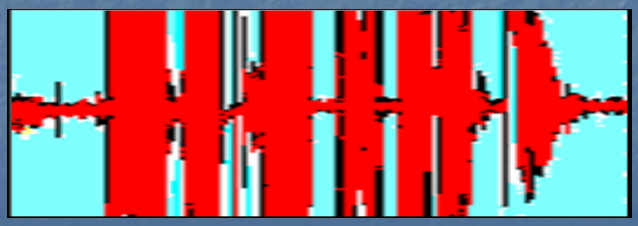


Iris Recognition - Issues

- Small target
- Moving target
- Located behind curved, wet, reflecting surface
- Obscured by lashes, lenses, reflections
- Partially occluded by (drooping) eyelids

Voice Verification

- Digitizes profile of a person's speech to produce a stored model voice, print or template
- Must be able to handle variations, distortions and noise in inputs from the real world.



Voice Verification

Reduces each spoken word to segments composed of several dominant frequencies or formants.

Extracts pitch, cadence, tone from digital sample to create the unique voice print which gets stored as a template

Voice prints are stored in databases in a manner similar to the storing of fingerprints or other biometric data

Voice Verification - Issues

- A person's speech is subject to change depending on health and emotional state. Matching a voice print requires that the person speak in the normal voice that was used when the template was created at enrollment.
- If the person suffers from a physical ailment, such as a cold, or is unusually excited or depressed, the voice sample submitted may be different from the template and will not match

Facial Recognition

Taking a 3D object and trying to make a comparison using a 2D image

Local Feature Analysis:

Looks at specific parts of the face that do not change significantly over time such as

- Upper sections of eye sockets
- Area surrounding the cheek bones
- Sides of the mouth
- Distance between the eyes

Facial Recognition

Eigenface Method:

Looks at the face as a whole

Collection of facial scans are used to generate a 2-D gray-scale image to produce a biometric template

Facial Recognition

- Identification – algorithm ids unknown face in an image by searching an electronic mugbook
- Verification – algorithm confirms claimed id of a particular face
- Research ongoing to improve accuracy of algorithms and decrease margins of error

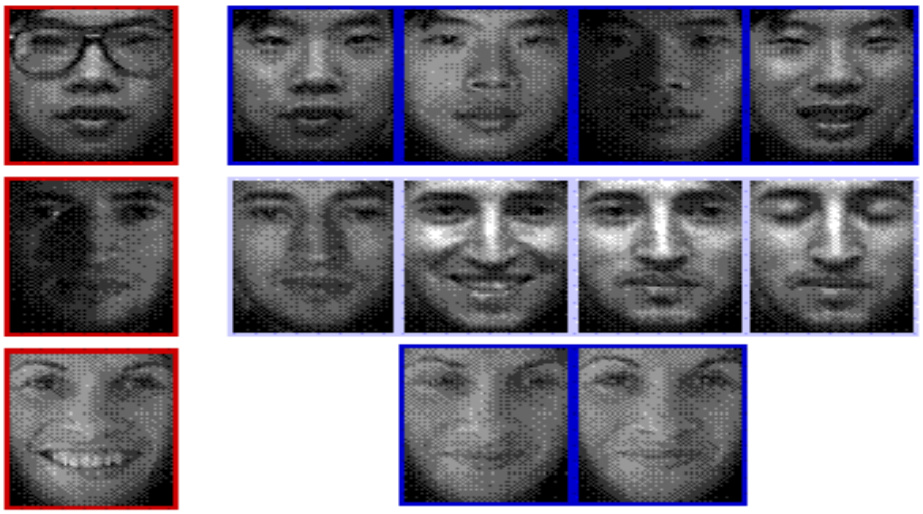


Figure 2. Successful queries (left) in ORNL system with complete training data (right). Note decoration (top), illumination (middle), and expression (bottom) variation in queries with respect to the corresponding training data.

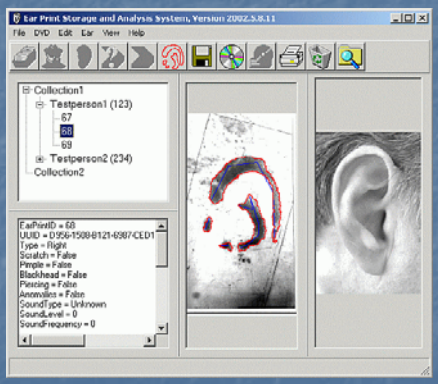
Facial Recognition - Issues

Susceptible to age, weight, fashion

- Can be affected by orientation (angle of image capture), clarity, lighting, etc
- Results are often based on similarities of class and individual characteristics
- Results produced based on probabilities
- Larger margin of error than other biometrics

Ear prints

- Amount of pressure used in making prints could affect ability to make reliable comparison
- Unique qualities e.g., wrinkles, lobe attachment



Lip prints

- External surface of the lip has many elevations and depressions forming a characteristic pattern called lip prints, examination of which is referred to as cheiloscopy
- arrangement of lines on the red part of the human lips is individual and unique for each human being. Lip print recording is helpful in forensic investigation that deals with identification of humans, based on lip traces.
- (Chicago Tribune article 3-10-06 Lavelle Davis case, lip prints on roll of duct tape)

Emerging Biometrics

Technology	How it works	Maturity
Vein scan	Captures images of blood vessel patterns.	Commercially available.
Facial thermography	Infrared camera detects heat patters created by the branching of blood vessels and emitted from the skin.	Initial commercialization attempts failed because of high cost.
DNA matching	Compares accrual samples of DNA rather than templates generated from samples.	Many years from implementation.
Odor sensing	Captures the volatile chemicals that the skin's pores emit.	Years away from commercial release.
Blood pulse measurement	Infrared sensors measure blood pulse on a finger.	Experimental.
Skin pattern recognition	Extracts distinct optical patters by spectroscopic measurement of light scattered by the skin.	Emerging.
Nailbed identification	An interferometer detects phase changes in back-scattered light shone on the fingernail; reconstructs distinct dimensions of the nailbed and generates a one-dimensional map.	Emerging.
Gain recognition	Captures a sequence of images to derive and analyze motion characteristics.	Emerging; requires further development.
Ear shape recognition	Is based on distinctive ear shape and the structure of the cartilaginous, projecting portion of the outer ear.	Still a research topic.

Future of Biometrics and the Courts

- Need better sensors – fake vs. real
- Improved image quality – sharper scans
- Combine biometric traits to improve accuracy – depending on conditions
- Better testing – minimize error margins

Dr. Anil Jain, Michigan State University

Future of Biometrics and the Courts

- Technologies have promise and are already in widespread practice in schools, airports, Homeland Security, etc.
- Just as polygraph is still widely used but not accepted in court, when biometrics are used to positively identify parties to a crime, they must satisfy the reliability of *Daubert*
- Validation studies to support the reliability of the techniques must be conducted for each discipline
- Databases of variations or "types" for each discipline should be constructed

THANK YOU!

Anjali R. Swienton, MFS, JD
301-528-5050
aswienton@scilawforensics.com
www.scilawforensics.com

SciLaw Forensics, Ltd.