Biometrics

Liability and Ethics Issues for Local Governments

IMLA Fall 2021

Cathy Cunningham
Senior Legal Editor
Thomson Reuters



I Love Technology

"The challenge facing the courts is that technology is outpacing the law."

In the Matter of the Search of a Residence in Oakland, California, 354 F.Supp.3d 1010 N.D. Cal. 2019)

But is it?



Topics include:

- What is Biometric Identifier
- Discussion of Major Identifiers
- Legal Issues with Public Safety
- Legal Issues with Employment Issues
- Other Legal Issues and Considerations
- Ethical Considerations

Types of Biometric Identifiers

Current use of the word biometrics refers to measurements of certain personal characteristics to verify a person's identity. Biometric identifiers include:

- Physical traits captured by:
  - Facial recognition technology (FRT);
  - Iris recognition or retina scans;
  - Fingerprints or palm prints;
  - DNA tests.
- Behavioral traits such as:
  - The way a person walks, also called their gait; and
  - Computer keystrokes.

Biometric Identifiers Do Not Include

- Tattoos.
- Height, weight, hair color, eye color, or other physical description.
- Demographic information.
- Writing samples or handwritten signature.
- Video or pictures (except for their use in FRT).

Fingerprints

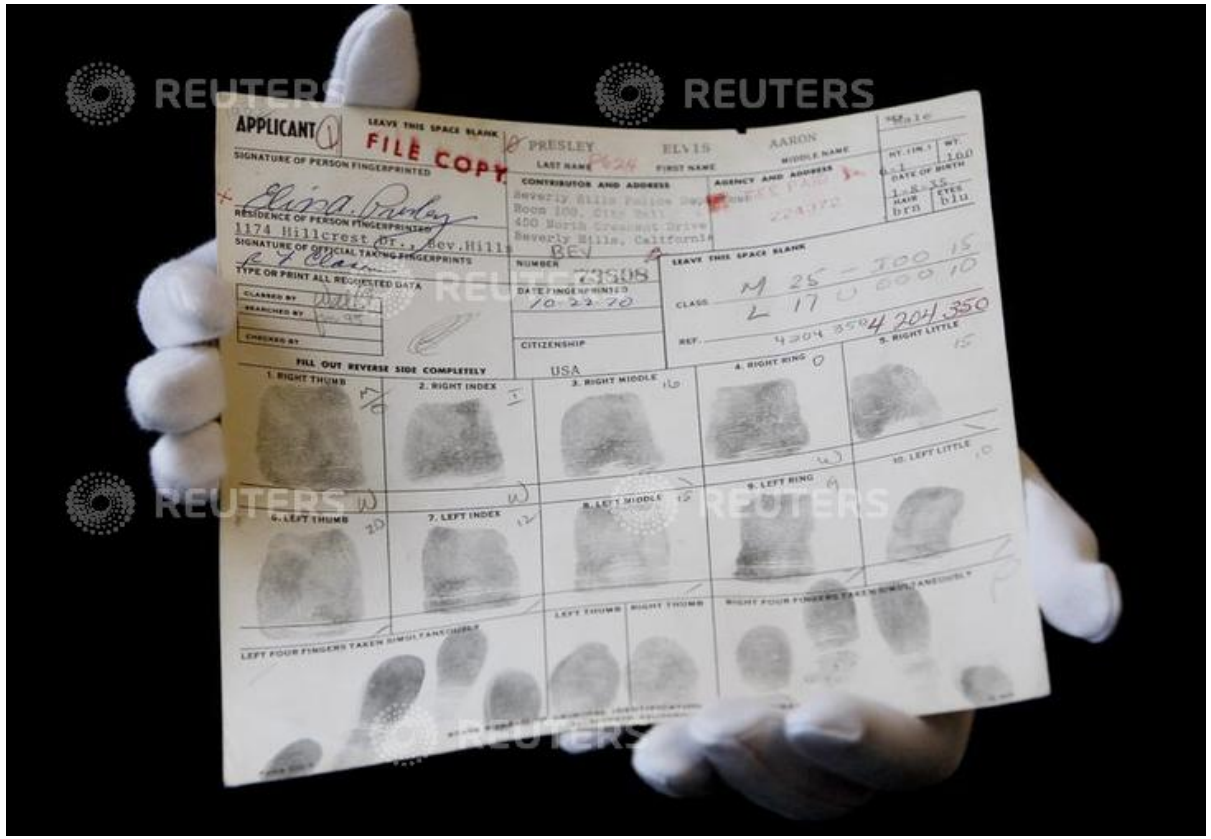
Scanned

Fingerprints



Inked prints

(Elvis Presley's)



History

- Classifying criminals can be traced back to at least as far as 1883, when Alphonse Bertillon created his system of criminal identification.
- He created three categories:
  - (1) descriptive data such as height, weight, and eye color;
  - (2) body marks such as scars, tattoos, and deformities; and
  - (3) body measurements.
- The categories were further divided into subcategories and it was difficult to use for large amounts of data. Use of the system ceased by the early 1900's.

History - Fingerprints

- The next development was for systems to analyze fingerprints.
- Systems included:
  - Dr. Johannes Purkinje (1787-1869) – developed nine classifications of fingerprint patterns (as well as being responsible for a large number and variety of medical discoveries).
  - Sir Francis Galton (1822-1911) – developed a classification for fingerprints. He was Charles Darwin's cousin and was also involved in several other scientific pursuits, including the discredited studies of eugenics. The phrase "Galton points" is still used for the places where the ridge lines stop or split (see *U.S. v . Mitchell*, 365 F.3d 215 (3d. Cir. 2004) at 221).
  - Dr. Henry Faulds (1843-1930) –developed the Henry system and the concepts of individuality and permanence. He was also a physician and participant in archaeologist excavations.
  - Juan Vucetich (1858-1925) –further subdivided the classifications of fingerprints. He was a police officer who successfully used fingerprints to prove a mother killed her two sons.
- The history is wildly incomplete, leaving out any number of people (such as Sir William Herschel), but providing a sense of the long timeline for biometrics

Fingerprint terminology (or the jargon the cool kids use)

- Points or Galton points – ridge endings, bifurcations, and other individual details.
- Latent (to lie hidden) print – A print not visible to the naked eye. Such prints usually have some distortions or other flaws due to dirt or grease (*U.S. v. Mitchell*, 2007 WL 1521212 (E.D. Pa. May 21, 2007).
- Rolled (Full) print – the print taken for identification where the fingerprint process starts on the side of the finger (near the fingernail) and is moved (rolled) to the other side.
- Plain or flat prints – the print taken for identification where the finger is placed flat on the surface (not rolled).
- AFIS – Automated Fingerprint Identification System
- IASIS – Integrated Automated Fingerprint Identification System
- III – Interstate Identification Index
- ACE-V - analysis, comparison, evaluation, and verification (*Fulgiam v. Kennedy*, 364 F. Supp. 3d 93 (D. Mass. 2019). Uses Level 1 to classify the type of print then Level 2 to identify Galton points and spatial relationships then Level 3 to determine deviations, breaks, scars, and similar details. The number of matching points occurs at Level 2.

Fingerprints –What is a Match

- “The standards used by the FBI at the evaluation stage of the ACE–V protocol are somewhat less concrete than the numerical descriptions found in television police dramas that extol “twenty-point matches” and the like. An *n*-point match refers to a match between an unknown latent print and a known full print in which the examiner has identified *n* corresponding Galton points in the correct geometry relative to one another.”
- France – 24
- Argentina and Brazil – 30
- UK, Canada - combination of quality and quantity, which can be subjective

U.S. v. Mitchell, 365 F.3d 215

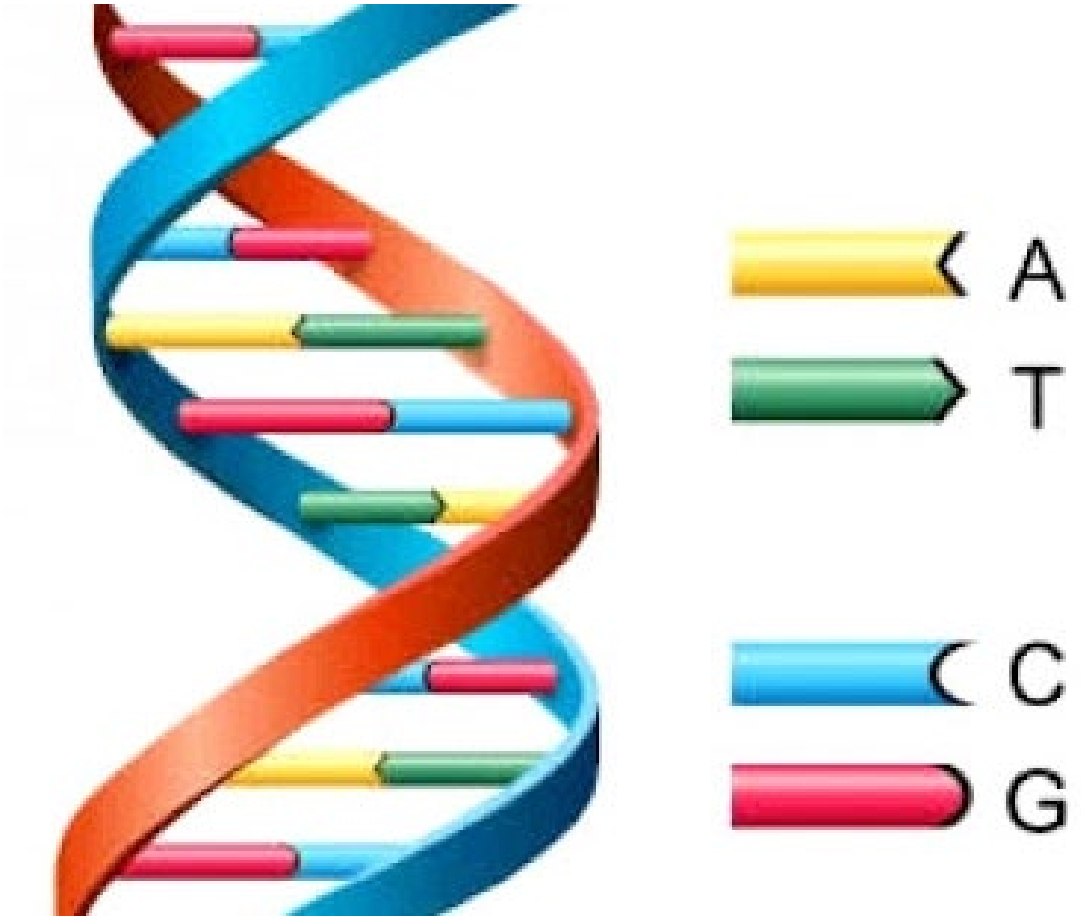
DNA

A –Adenine

C – Cytosine

G – Guanine

T - Thymine



DNA

- Deoxyribonucleic acid (DNA) is a two-strand double helix molecule found in a cell's nucleus.
- The cell must have a nucleus to have DNA (mature red blood cells lose their nucleus to be able to carry more oxygen).
- DNA consists of four bases, adenine (A), cytosine (C), guanine (G), and thymine (T) referred to as ACGT.



DNA

- DNA from a crime scene is examined to compare and possibly match DNA in the Combined DNA Index System (CODIS).
- The DNA from certain specific locations (locus or loci) is used.
- Tests check for the alleles (genes) at those sites.
- Rapid DNA is an on-site automated system that identified DNA. Information from a buccal (cheek) swab can be entered but at this time, Rapid DNA is not used for testing crime scene samples.

Facial Recognition Technology



Facial Recognition Technology



- Facial recognition technology is one of the newer types of biometric technology in common use.
- The first step in facial recognition technology is enrolling an image, which involves:
  - Capturing the image of a face (taking a picture);
  - Converting the image; and
  - Storing the image for possible future comparison and match.

Facial Recognition Technology

- The technology converts images by using nodal points on a face to gather numeric information (such as the distance from one point to another point or the angle between points) to create a numeric code that is a faceprint.
- The image of a face is mapped using an algorithm that embeds recognition points into the image.
- To detect someone, the technology uses algorithms to compare that face (the probe) to the previously stored images.
- The matches are usually rated by percentage (a 60% match, for example).

Facial Recognition Technology

- Facial recognition technology (FRT) is not one technology, and it is not one algorithm. There are multiple algorithms and systems and multiple companies that provide FRT.
- As the technology continues to develop, there has been some exploration of combining FRT with the use of police worn body cameras.



Facial Recognition Technology
One-to-One; One-to-Many

- Often the types of FRT usages are referred to as either one-to-one or one-to-many.
- One-to-one usage is used to recognize and unlock a cell phone or computer for the authorized user. One-to-one is used by individuals or companies to authorize usage of a device.
- One-to-many is the method used by law enforcement. A picture (the probe image) is compared with existing photos in the databank, which means that one probe image is used and the databank supplies multiple responses.

Use of Facial Recognition Technology by Law Enforcement

- Law enforcement generally does not use FRT to identify or eliminate a suspect (*People v. Carrington,* 2018 WL 671903 (Cal. App. February 2, 2018 noncitable)).
- Law enforcement use of FRT includes use to:
  - Generate suspect leads.
  - Identify victims.
  - Confirm the disappearance of victims (*Nisbett v. State,* 552 S.W. 3d 244 (Tex. Crim. App. 2018)).
  - Support other evidence presented.

Reliability and Bias in Facial Recognition Technology

- There have been reports and lawsuit claims that FRT has higher rates of false positives for certain Black, Asian, and Native groups and for females.
- The error rate is dependent on the algorithm used. Some algorithms perform better than others "and those that are the most equitable also rank among the most accurate. This last point underscores one overall message of the report: Different algorithms perform differently." (NIST Study Evaluates Effect of Race, Age, Sex on Face Recognition Software.)

Reliability and Bias in Facial Recognition Technology

- In addition to the effect of the algorithm on the performance of FRT, other factors include:
  - The quality of the probe photo. (Important point: do not use someone else's photo just because the probe photo is not great and the other person "looks a lot like" the probe photo. The computer uses math, not looks!)
  - The size of the database used.

Reliability and Bias in Facial Recognition Technology

- The NIST has released "A Proposal for Identifying and Managing Bias Within Artificial Intelligence" to address these issues for Artificial Intelligence (AI) generally. Establishing trustworthy standards for AI helps establish more reliable standards for FRT.
- NIST proposal: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270-draft.pdf

Other Types of Biometric Identifiers

- Iris Recognition
- Retina Scan
- Voice Identification



Iris Recognition and Retina Scans

- Iris recognition uses an automated system that identifies the unique pigmentated portion of the eye.
- Retina scans use equipment which examines the blood vessels in the retina.
- Both require a subject to be close to the equipment.



Voice Recognition

- Voice recognition can be done by a person or a technology.
- Before *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, expert testimony on aural spectrographic voice identification was allowed (509 U.S. 579 (1993)). However, since *Daubert* "no federal court has accepted such voice identification evidence" (*United States v. Mills*, 2021 WL 2351114 (3d Cir., June 9, 2021)).

(Pictured – Raytron's communication robot Chapit)



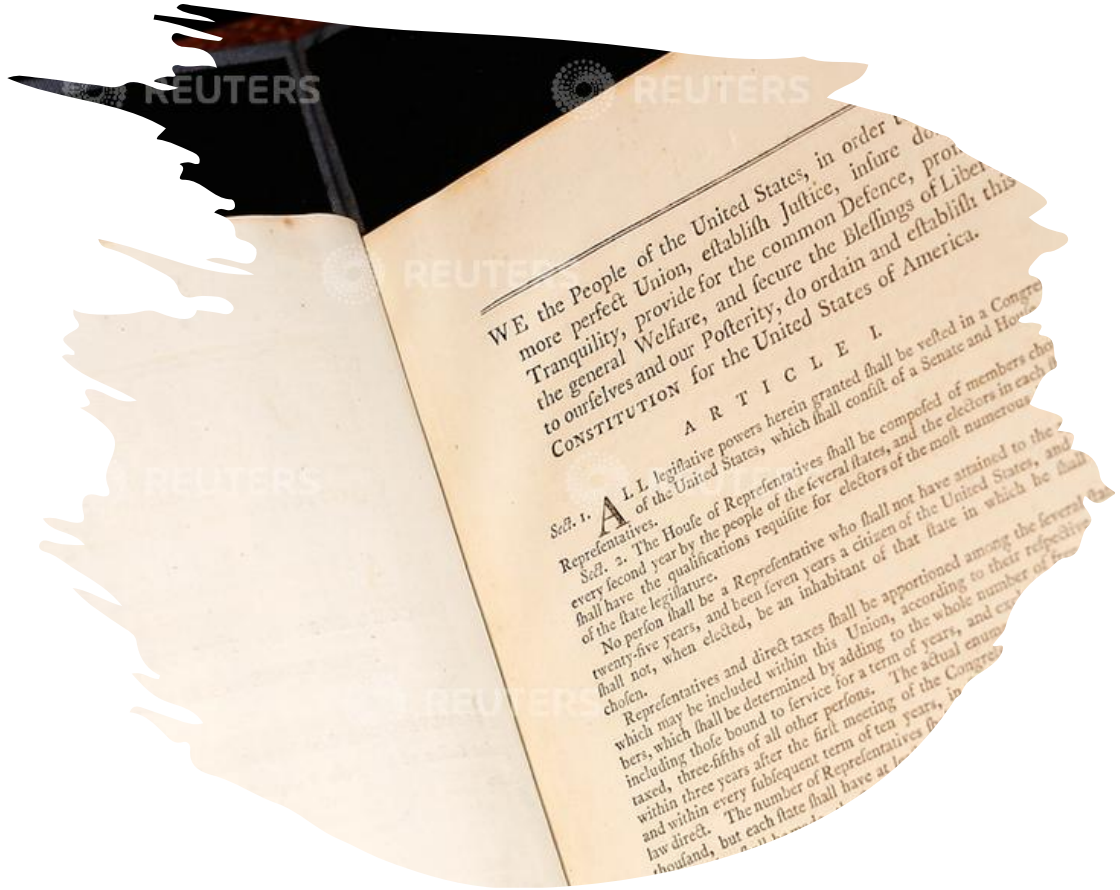
Legal Issues
Biometrics and Public Safety





Legal Issues – Potential Claims - Law Enforcement Use
Constitutional Challenges

- Fourth Amendment claims that using biometric identifiers is an unlawful search or seizure.
- Fifth Amendment claims that the use of biometric evidence forces criminal defendants to incriminate themselves.
- Sixth Amendment claims that the introduction of biometric evidence violates defendants' right to confront the witnesses against them.



Legal Issues – Potential Claims - Law Enforcement Use
Reliability in Federal Courts

Federal courts review the following factors to determine admissibility of expert testimony concerning scientific evidence, such as fingerprint evidence, DNA, or FRT:

- Testability.
- Peer review.
- Error rate.
- Maintenance of standards.
- General acceptance.
- Relationship to established reliable techniques.
- Qualifications of the expert.
- Non-judicial use of the technique, that is, that the techniques used are relied on outside of court.

Legal Issues – Potential Claims - Law Enforcement Use
Reliability in State Courts

- Most state courts follow the same standards set out in *Daubert*. Some states still use the *Frye* standard (*Frye v. United States*, 293 F. 1013 (D.C. Dir. 1923)).
- For more information about expert testimony in state court, there is a Practical Law resource “Standard for Excluding Expert Testimony: 50 State Survey.”

Legal Issues – Potential Claims - Law Enforcement Use
Reliability

- The National Institute of Standards and Technology (NIST) provides standards for biometric technology.
- They also partner with the American National Standards Institute (ANSI) to provide standards as part of work at the Information Technology Laboratory (ANSI/NIST-ITL).

Cases –Fingerprints - Public Safety

Fourth Amendment

- The Fourth Amendment does not prohibit fingerprinting a person.
- However, police officers cannot detain someone just to take their fingerprints. (*Hayes v. Florida*, 470 U.S. 811 (1985).)
- To use a fingerprint to unlock a cell phone requires a warrant (*Riley v. California*, 573 U.S. 373 (2014)).



Cases - Fingerprints
Public Safety

Fifth Amendment

- Courts traditionally held that the Fifth Amendment "offers no protection against compulsion to submit to fingerprinting, photography, or measurements, to write or speak for identification, to appear in court, to stand, to assume a stance, to walk, or to make a particular gesture" (*United States v. Wade*, 388 U.S. 218, 223 (1967)).
- However, when fingerprints are compelled to unlock a cell phone, court decisions have been mixed, holding that a fingerprint:
  - was testimonial (*In the Matter of the Search of a Residence in Oakland, Cal.,* 354 F. Supp. 3d 1010 (N.D. Cal. 2019));
  - was not testimonial (*Matter of Search Warrant Application for cellular telephone in United States v. Barrera*, 415 F. Supp. 3d 832 (N.D. Ill. 2019))

Cases - Fingerprints
Public Safety

Sixth Amendment and Hearsay Objections

Admission of fingerprints does not violate the Sixth Amendment and is not hearsay. "Because there was no human declarant, there was no out-of-court statement to be offered for its truth, and therefore no hearsay." (*Robertson v. Keyser*, 2021 WL 2453939 (E.D. N.Y. June 16, 2021).

Cases - Fingerprints
Public Safety

Privacy Objections to Fingerprints

- A state or local government that lawfully obtains a person's fingerprints does not violate privacy rights. "To the extent Plaintiff claims that SRCSO violated her right to privacy by 'unlawfully' taking her fingerprints, Plaintiff has failed to state a claim." (*Wickers v. Utsey*, 2008 WL 4999247 (N.D. Fla. November 20, 2008).)
- However, if a local government wishes to establish a fingerprint requirement for a licensing procedure, there must be some evidence that the requirement furthers the legitimate interests of the local government (see *Pac. Frontier v. Pleasant Grove City*, 414 F.3d 1221 (10th Cir. 2005)).

Cases - DNA
Public Safety

- **Fourth Amendment**: The police may take a buccal swab of an arrestee to obtain and analyze the arrestee's DNA as part of the procedure used for booking someone into jail. Processing the DNA sample and entering it into CODIS is not an unconstitutional search (*Maryland v. King*, 569 U.S. 435 (1994)).
- **Fifth Amendment**: Taking a prisoner's DNA does not violate the Fifth Amendment because DNA samples are not testimonial (*Boling v. Romer*, 101 F.3d 1336 (10th Cir. 1996)).
- **Sixth Amendment:** A criminal defendant's Sixth Amendment right to confront witnesses is not violated by expert testimony about DNA laboratory tests (*Williams v. Illinois*, 567 U.S. 50 (2012)).

Cases - Facial Recognition Technology
Public Safety

Fourth and Fifth Amendments

In *Carpenter v. United States*, the Supreme Court found only a Fourth Amendment violation in the search of a cell phone without a warrant and did not reference a Fifth Amendment violation (138 S. Ct. 2206 (2018)).



Cases - Facial Recognition Technology Public Safety

Fourth and Fifth Amendments

- One court found that unlocking a cell phone without a warrant by using the built-in FRT or iris recognition violates the Fourth and Fifth Amendment. The court found that even if the search was allowed under the Fourth Amendment, "probable cause does not permit the Government to compel a suspect to waive rights otherwise afforded by the Constitution, including the Fifth Amendment right against self-incrimination" (*Matter of Residence in Oakland, Cal.*, 354 F. Supp. 3d 1010, 1014 (N.D. Cal. 2019)).

- However, other courts differ, finding that evidence seized under a valid search warrant does not violate the defendant's Fifth Amendment rights against self-incrimination. (*Bradley v. Cheshire*, 2020 WL 6684995 (D. Del. November 12, 2020).)

- In the warrant application, police can request the "'authority to compel [defendant] to provide a biometric key (facial recognition or thumbprint) to unlock' the cellphone at issue" (*United States v. Maffei*, 2019 WL 1864712 (N.D. Cal. April 25, 2019)).



Cases - Facial Recognition Technology Public Safety

Sixth Amendment

- Criminal defendants have also claimed that the failure of law enforcement to use FRT resulted in a Sixth Amendment speedy trial violation. The argument is that if law enforcement had used FRT, the defendant may have been caught sooner, so the failure to use it caused a delay in the defendant's trial. Because the defendant was actively evading capture, the court denied the defendant's motion to dismiss. (*United States v. Lazzara*, 709 Fed. Appx. 578 (11th Cir. 2017).)
- Also, in *Maffei*, the court allowed the use of biometrics (and did not support the Fourth and Fifth Amendment claims) but the court suppressed the defendant's statement about the defendant's passcode as violating the Sixth Amendment right to counsel.

Cases - Iris Scans

Public Safety

Fourth Amendment Objections to Iris Scans

- Iris scans are allowed as a routine administrative step at time of arrest (*Morgan v. City of New York*, 2021 WL 2207002 (E.D.N.Y March 25, 2021)).

Fourteenth Amendment Objections to Iris Scans

- Neither the iris scan nor a short delay in the arraignment process attributable to the iris scan violate the Fourteenth Amendment or substantive due process (*Leibowitz v. City of New York*, 2014 WL 772349 (S.D.N.Y. February 25, 2014)).

Reliability of Fingerprints

- Fingerprints: Found to be reliable (*United States v. Mitchell*, 365 F.3d 215 (3d Cir. 2004)).
- DNA: Courts have found short tandem repeats (STR) DNA tests reliable (*United States v. McCluskey*, 954 F. Supp. 2d 1224 (D.N.M. 2013)).

Reliability of Facial Recognition Technology

- Reliability of Facial Recognition Technology: Evolving. There are fewer reported lawsuits involving FRT.
- Many of the cases about FRT do not concern public safety and are more likely to be about patents and copyrights.
- Reliability issues include possible bias in the algorithms used.
- The technology is used to generate leads and not for a final identification or to support other evidence. Due to the limited role, the prosecution may not offer FRT as evidence, so there may not be a ruling on its admissibility.

Reliability of Iris Scans

Reliability of Iris Scans: "Iris scans are high resolution photographs of the pigmented portion of the eye, and are more accurate than fingerprints in confirming identity." (*Leibowitz v. City of New York*, 2014 WL 772349 (S.D.N.Y. February 25, 2014).)



Cases – The Crazy People

Pro Se and Sovereign Citizen Claims

Some pro se and sovereign citizen lawsuits make a variety of claims against the government in regard to biometrics, including:

- A Fifth Amendment takings case concerning taking the plaintiff's fingerprints, a retina scan, and the plaintiff's energy. The case was dismissed. (*Davenport v. United States*, 2017 WL 5988354 (Cl. Ct. Dec. 4, 2017).)
- Claims that multiple cities, federal, state, and local agencies, and officials violated the plaintiff's civil rights claiming that they used facial recognition software to track the plaintiff's movements (as well as stealing the plaintiff's ideas using wiretaps and that they intercepted and impugned the plaintiff's financial transactions and other bizarre claims). The case was dismissed. (*Brown v. U.S. Dept. of Defense*, et al., 2019 WL 3023367 (N.D. Tex. July 2, 2019).)

Prisoner Lawsuits and *Heck* Doctrine

- A person may challenge the use of biometric evidence against them at their criminal trial or as a plaintiff in a civil trial. A person cannot invalidate a criminal conviction using a Section 1983 or other civil claim for damages.
- "We hold that, in order to recover damages for allegedly unconstitutional conviction or imprisonment, or for other harm caused by actions whose unlawfulness would render a conviction or sentence invalid, a § 1983 plaintiff must prove that the conviction or sentence has been reversed on direct appeal, expunged by executive order, declared invalid by a state tribunal authorized to make such determination, or called into question by a federal court's issuance of a writ of habeas corpus, 28 U.S.C. § 2254." (*Heck v. Humphrey*, 512 U.S. 477 (1994)





Black Box Problem

- The local government should be prepared to explain the use of the technology in analyzing biometrics at a level that a judge or jury can understand. People mistrust technology when they cannot understand how it works and cannot decide for themselves how accurate it is.
- The "black box" problem refers to the view of some members of the public that technology is confusing and cannot be trusted. Their perception of biometric technology is that a question is entered into an opaque box and an answer pops out, with no rational explanation of the process.



Black Box Problem Continued

- The problem is not limited to biometrics and includes other technologies, such as Artificial Intelligence (AI).
- A court's inability to review the findings from technology weighs against the party using the technology.
- When purchasing and using this technology, a local government should acquire and use technology that can be explained, either by their staff or by the vendor or other experts. A local government should include this requirement in its specifications (requests for bids or requests for proposals (RFP)) and in the contract.

Employment Issues and Biometrics







Employment Issues and Biometrics

Like other employers, local government employers may use biometrics for:

- Physical security and access to the work site.
- Electronic security and access to an employer owned networks, computer systems, data, and other electronic systems or information.
- Attendance and timekeeping.
- Immigration compliance.
- COVID screening (temperature checks).

Employment Issues and Biometrics

Potential causes of action that may arise from use of biometric technology in the workplace includes:

- Genetic Information Nondiscrimination Act (GINA) (42 U.S.C. §§ 2000ff-11).
- Religious discrimination under the First Amendment and, Civil Rights Act of 1964 (423 U.S.C. §§ 2000e).
- Age Discrimination in Employment Act (29 U.S.C. §§ 621-634).
- Electronic Communications Privacy Act, which includes Stored Communications Act (18 U.S.C. §§ 2701-2712), the Wiretap Act (18 U.S.C. §§ 2510-2522), and the Pen Register and Trap and Trace Devices Statute (18 U.S.C. §§ 3121-3127).
- State law claims, including unlawful acquisition or retention of biometric identifiers or improper destruction.

Employment Issues and Biometrics - GINA

- GINA prohibits employers from discriminating based on an employee's genetic information.
- Genetic information includes genetic tests or disease or disorder manifestation of the employee or a family member of the employee.
- Genetic information does not include ordinary medical information, for example, information needed in a fitness for duty examination (*Franks v. City of Austin*, 2020 WL 3446164 (W.D. Tex. June 24, 2020)).
- If the employer has any genetic information, it is confidential.
- GINA claims are often filed together with Americans with Disabilities Claims, age discrimination claims, and claims for retaliation.



Employment Issues and Biometrics - GINA

Exceptions to GINA include:

- Accidental acquisition of genetic information.
- Receipt of information given voluntarily in a wellness program.
- Request for information necessary to meet the requirements of the Family and Medical Leave Act, other state or local laws, or some employer leave policies.
- Acquisition of publicly available information.
- Genetic monitoring required by law or provided voluntarily (such as monitoring possible workplace toxins).
- DNA analysis for law enforcement purposes.



Employment Issues and Biometrics Religious Discrimination

- Local governments should explore alternatives if an employee has a sincerely held religious belief that conflicts with the use of biometric data.
- In one case, a city instituted new security procedures, including new security cards. The cards required employees to be fingerprinted. One employee complained that that fingerprints were the mark of the beast. The city fired the employee. The court found that the city should have explored possible accommodations. (*Craig v. City of New York*, 2007 WL 9712108 (E.D.N.Y. September 4, 2007).)

Employment Issues and Biometrics
Age Discrimination

- Fingerprints are sometimes less visible as people age.
- In addition to the passage of time, exposure to chemicals, work that involves use of hands, and other factors may cause fingerprints to diminish.
- If a workplace requires fingerprints for computer usage, building entry, or other uses, the biometric system may have more difficulty reading an older person's fingerprints.
- An employer should consider offering alternative means of access.

Employment Issues and Biometrics

- The Stored Communications Act (part of the Electronics Communications Privacy Act) was passed to protect the privacy of electronic communications while in electronic storage.
- Some plaintiffs claim that biometric tracking, use, or storage violates the Stored Communications Act.





Employment Issues and Biometrics

Court decisions vary about whether keystroke monitoring violates federal law:

- Use of keystrokes or keylogger programs is not a violation of the Stored Communications Act. (*Langston v. Langston*, 2011 WL 4007338 (E.D. Tex. August 31, 2011).)
- Keystrokes not covered by Electronic Communications Privacy Act (*United States v. Scarfo*, 180 F. Supp. 2d 572 (D.N.J. 2001)).
- Keystrokes may be covered (*Brahmana v. Lembo*, 2009 WL 1424438 (N.D. Cal. May 20, 2009)).

Employment Issues and Biometrics State Laws

- The types of actions are evolving and include claims about acquisition, misuse, retention, or improper destruction of biometric identifiers.
- The state law claims usually have government or public safety exceptions, but these causes of action **emphasize the importance of not agreeing to defend or indemnify any vendors** in contracts for this technology (see Contract Issues).
- Some states have directly passed legislation addressing biometric identifiers, in other states, laws about consumer protection, medical privacy, or personally identifiable information may also cover biometric issues.



Employment Issues and Biometrics State Laws

Examples of plaintiffs' claims include:

- Failure to maintain and provide a written policy about biometric information.
- Failure to provide written notice and obtain written consent before acquiring or retaining biometric information.
- Improper acquisition of biometric information.
- Improper sale or distribution of biometric information.
- Failure to properly transmit biometric information.
- Failure to safely store and protect biometric information.
- Failure to properly destroy biometric information.

Biometrics and Discovery Issues

- Discoverable information may exist on a device that uses a biometric identifier, for example, text messages on a cell phone that unlocks with facial recognition.
- A party can ask that a court require the opposing party provide biometric identifiers in evidence preservation orders. (*Solar Connect, LLC v. Endicott*, 2018 WL 2386066 (D. Utah April 6, 2018))



Biometrics and Contracts Issues

- Many lawsuits concerning biometric identifiers arise in the areas of either patents under federal law or use and retention by businesses under state law.
- The local government is usually not involved in either of these areas.
- However, a bad contract provision may subject a local government to claims in these areas if the local government agreed to insure or indemnify the vendor.



Biometrics and Contracts Issues, continued

- It is always important that a local government **not** agree to assume a duty to defend or to indemnify other parties to a contract, but it is especially important in contracts with vendors of biometric products.
- Vendors are subject to more causes of action than local governments, especially under many states' laws. Agreeing to defend or indemnify a vendor in a contract, even if those clauses are not valid, creates additional problems for local governments.

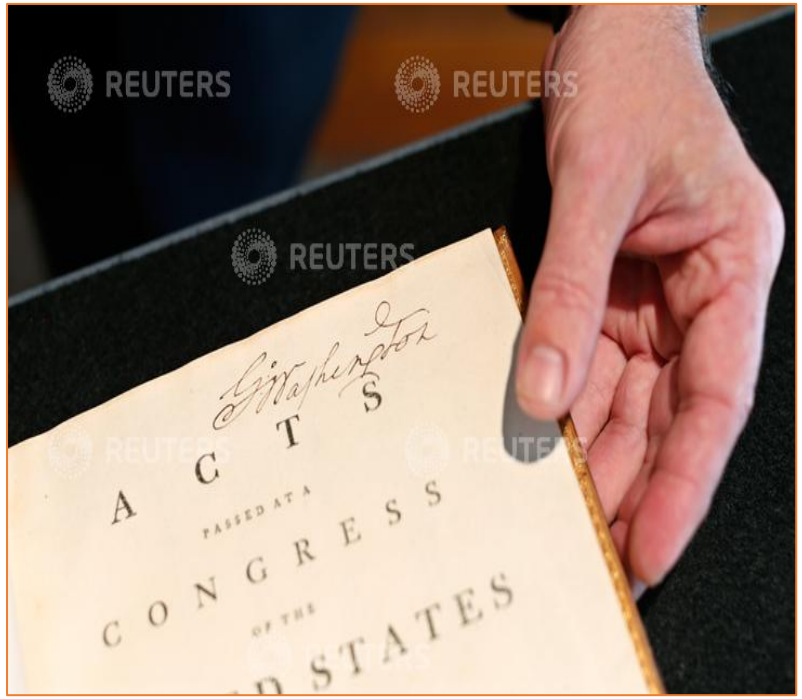


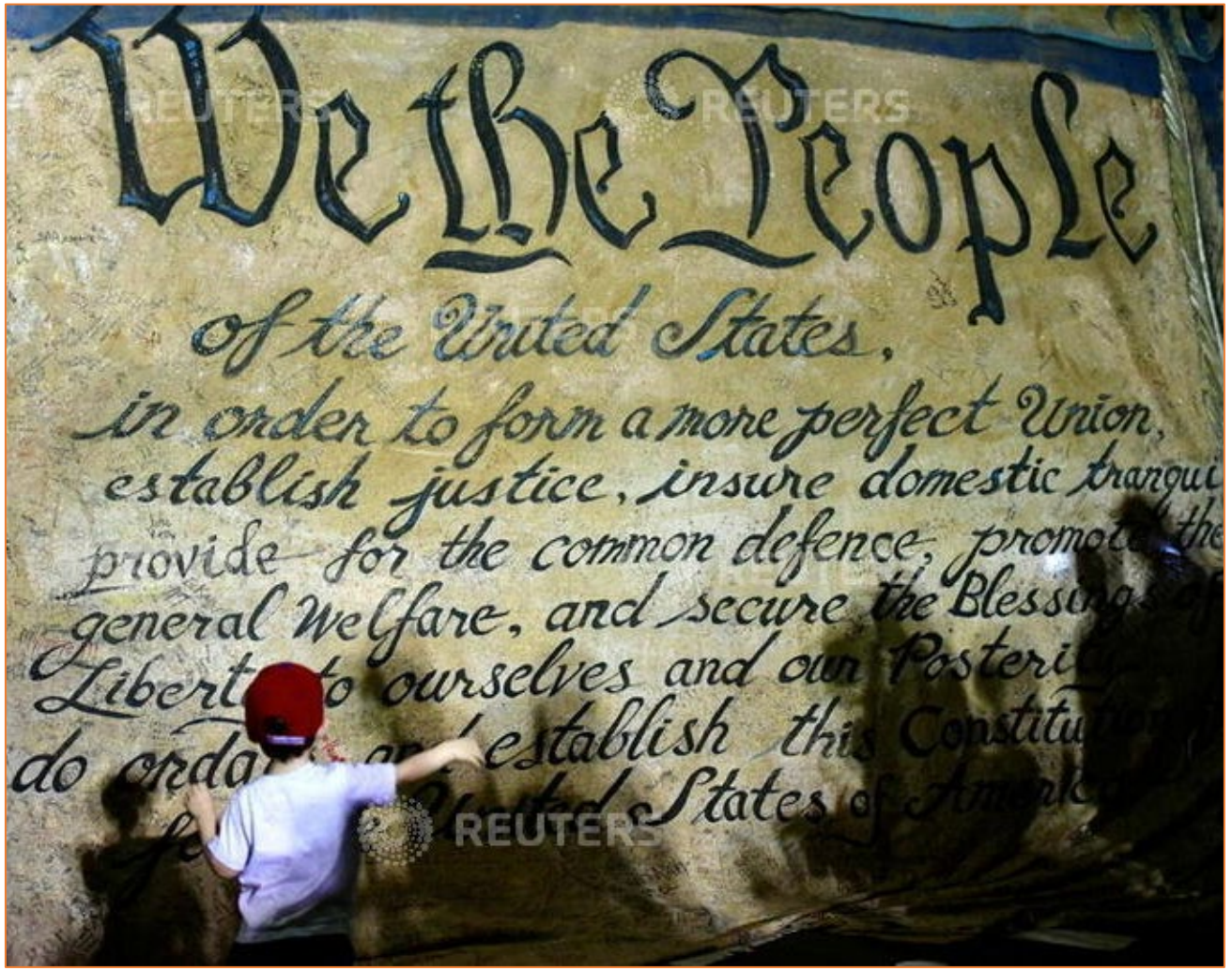
Biometrics and Public Records

- All states have statutes allowing access to public records.
- However, if a local government receives a request for an individual's biometric identifiers, the local government personnel should check for exemptions to release and the procedure for asserting these exemptions.
- The exemptions may not be within the public records statute. For example, in Texas the Public Information Act is found in Tex. Gov't Code Ann. §§ 552.001-552.353, but the exception for biometric information is found in Tex. Gov't Code Ann. §§ 560.002-560.003



Ethics, AI, & Biometrics







Attorney Ethics and Biometrics

Just to show that the law is keeping up, there are applications from the ABA Model Ethical Rules that apply:

- ABA Rule 1.1.
- ABA Rule 3.8.
- ABA Rule 4.4.
- ABA Rule 5.3.



Ethics, AI, and Biometrics

- **Rule 1.1**
- "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."
- Comment 8 "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject."

Ethics, AI, and Biometrics

Rule 3.8 Special Responsibilities Of A Prosecutor

- “The prosecutor in a criminal case shall: (a) refrain from prosecuting a charge that the prosecutor knows is not supported by probable cause;”

- Comment [1]: “A prosecutor has the responsibility of a minister of justice and not simply that of an advocate. This responsibility carries with it specific obligations to see that the defendant is accorded procedural justice, that guilt is decided upon the basis of sufficient evidence, and that special precautions are taken to prevent and to rectify the conviction of innocent persons.”



Ethics, AI, and Biometrics

Rule 4.4

"Transactions With Persons Other Than Clients

(a) In representing a client, a lawyer shall not use means that have no substantial purpose other than to embarrass, delay, or burden a third person, or use methods of obtaining evidence that violate the legal rights of such a person.

(b) A lawyer who receives a document or electronically stored information relating to the representation of the lawyer's client and knows or reasonably should know that the document or electronically stored information was inadvertently sent shall promptly notify the sender."

Biometrics and Disciplinary Rules

Rule 5.3: Responsibilities Regarding Nonlawyer Assistance

"With respect to a nonlawyer employed or retained by or associated with a lawyer: . . . .

(b) a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and

(c) a lawyer shall be responsible for conduct of such a person . . ."

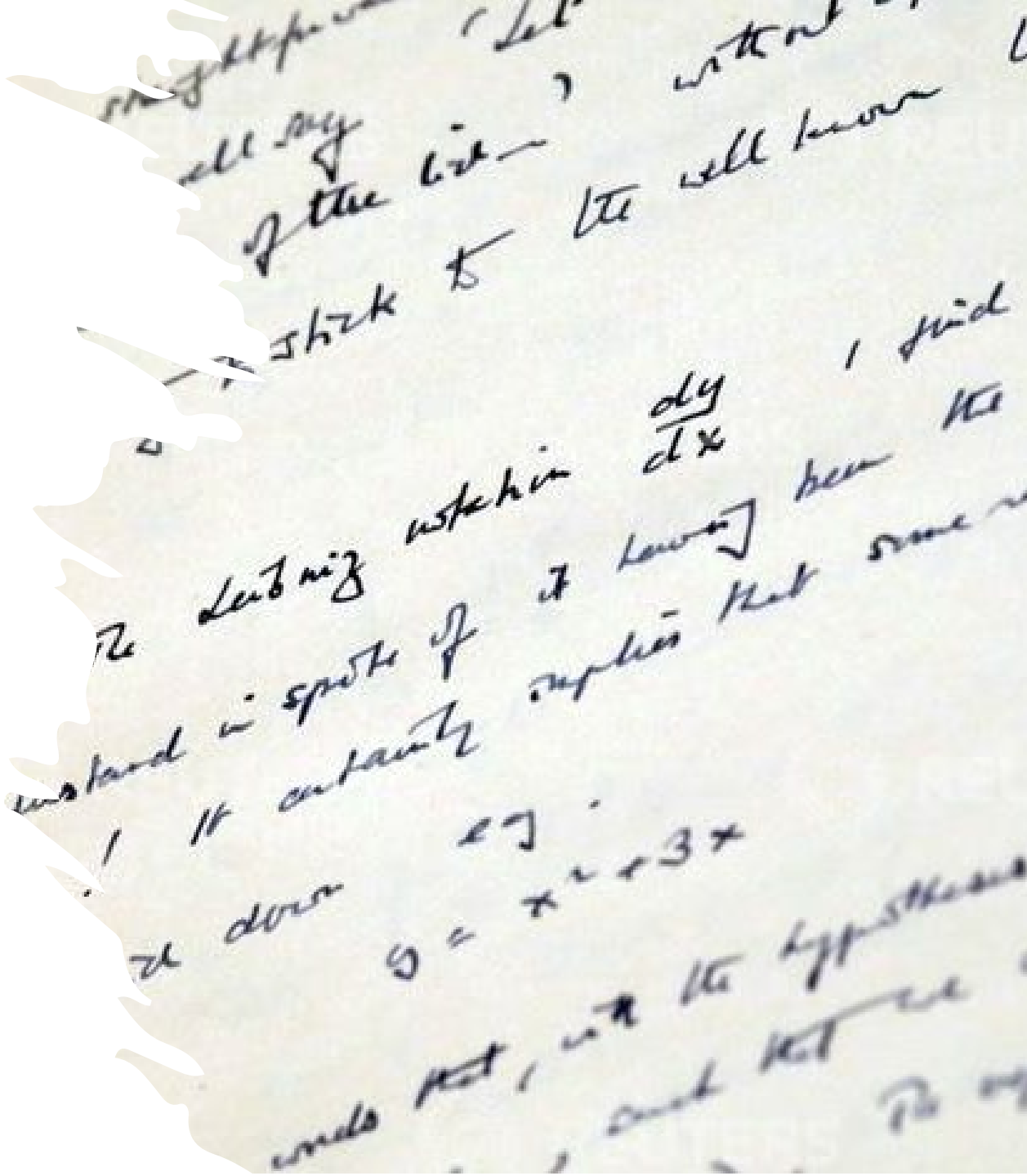
For example- your IT staff?

Computers Do Not Think Like We Do: A Mathematical Formula for Trust

"There are, at the time of this writing, nine identified characteristics that define an AI system's trustworthiness:

- Accuracy,
- Reliability,
- Resiliency,
- Objectivity,
- Security,
- Explainability,
- Safety,
- Accountability, and
- Privacy. From an engineering perspective, an AI system needs these characteristics if it is to be trusted."

From *Trust and Artificial Intelligence*, by Brian Stanton and Theodore Jensen https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8332-draft.pdf



Comments or Questions?

Cathy Cunningham

cathy.cunningham@thomsonreuters.com

Or

cathy.cunningham@tr.com

469-583-0926

www.linkedin.com/in/cathy-cunningham-301b659

