THOMSON REUTERS
PRACTICAL LAW™

Biometrics and Local Government Issues

by Practical Law Government Practice

Status: **Maintained** | Jurisdiction: **United States**

This document is published by Practical Law and can be found at: **us.practicallaw.tr.com/w-031-5970**
Request a free trial and demonstration at: **us.practicallaw.tr.com/about/freetrial**

A Practice Note providing guidance to local governments on issues concerning biometric identifiers for both law enforcement purposes and in the employer-employee relationship. The Note discusses various biometric identifiers, including fingerprints, DNA testing, facial recognition technology, and others. It reviews various claims regarding biometric technology, such as constitutional claims including Fourth Amendment, Fifth Amendment, and Sixth Amendment, and reliability issues. This Note covers employment issues, including GINA, age discrimination, religious discrimination, and state law claims.

Biometric information technology, such as facial recognition technology, voice recognition, iris recognition and retina scans, DNA testing, fingerprints, palm prints, keystrokes, and other identifiers, provide local governments with useful information for public safety and employee monitoring. However, some people object to the use of biometric identifiers. This Note addresses legal issues about use of biometric identifiers by local government.

This Note does not address issues or uses of biometric identifiers by:

- The military.
- Healthcare providers or companies.
- Immigration enforcement.
- Commercial companies.

Types of Biometric Identifiers

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

- Physical traits captured by:
  - facial recognition technology (FRT);
  - iris recognition or retina scans;
  - fingerprints or palm prints; and
  - 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

Fingerprints refer to the corrugated surfaces (called friction ridges) on the skin of a person's fingers, hands, and parts of their feet. The friction ridges create the appearance of lines (from the high points) and white spaces (from the low points) that appear on people's fingerprints.

Fingerprints left on a surface "are nothing more than an impression of the friction ridges on the fingertip (and palm) that result when oil is deposited upon contact with a surface" (*United States v. Mitchell*, 2007 WL 1521212 (E.D. Pa. May 21, 2007)).

Because fingerprints are unique (even identical twins do not have the same fingerprints) and permanent, they identify who put the fingerprints on an object.

© 2021 Thomson Reuters. All rights reserved. Use of Practical Law websites and services is subject to the Terms of Use (static.legalsolutions.thomsonreuters.com/static/agreement/westlaw-additional-terms.pdf) and Privacy Policy (a.next.westlaw.com/Privacy).

DNA

Deoxyribonucleic acid (DNA) is a two-strand double helix molecule found in a cell's nucleus. It contains the organism's genetic information. DNA consists of four bases, adenine (A), cytosine (C), guanine (G), and thymine (T), referred to as ACGT. Although DNA is made of the same components, DNA is unique to each person, which makes it useful for identification in criminal cases.

For suspect identification, the forensic scientist looks at DNA found in certain specific places (called locus or loci) on the molecule. The FBI lists those loci used in forensic tests. Tests check for the occurrence of certain alleles (genes) at those sites. "The alleles at comparable loci vary from person to person and are the basis of individual DNA profiles" (*United States v. Jones*, 965 F.3d 149, 155 (2d Cir. 2020)).

DNA from crime scenes is examined for the purposes of comparing and possibly matching it with DNA in the Combined DNA Index System (CODIS). CODIS is a federal, state, and local database with more than 20 million DNA profiles. At this time, the DNA obtained is not used to determine other traits (such as appearance or disease). DNA is entered into the system from swabs that come from known reference samples (arrested persons). Those swabs are not contaminated the way samples may be from a crime scene.

Rapid DNA

Rapid DNA refers to an on-site, automated system that identifies DNA. At this time, the FBI allows information from a rapid test using a buccal (cheek) swab to be entered into the CODIS infrastructure. At this time, rapid DNA is not approved for testing crime scene samples.

Facial Recognition Technology

Facial (or face) recognition technology, also called FRT, is one of the newer types of biometric technology in common use.

The first step of FRT is enrolling an image, which involves:

- Capturing the image of a face (taking a picture).
- Converting the image.
- Storing the image for possible future comparison and match.

The technology converts images by using nodal points on a face to gather numeric information (distance from one point to another or the angle between points) to create 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 other previously stored images. The matches are usually rated by percentage, for example, a 58% match.

Facial recognition technology is not one technology. There are multiple algorithms and systems and many companies that provide FRT. For example, the FBI uses two systems:

- The Next Generation Identification-Interstate Photo System (NGI-IPS).
- The Facial Analysis, Comparison, and Evaluation (FACE).

As the technology develops, there has been some exploration of combining FRT with the use of police worn body cameras.

One-to-One; One-to-Many

Often the types of FRT usages are referred to as either one-to-one or one-to-many.

An example of a one-to-one usage is using facial recognition to unlock a cell phone. A local government may employ a one-to-one usage in its capacity as an employer, for example, to unlock an assigned city computer.

A one-to-many is the method used by law enforcement. When law enforcement compares a picture (probe image) with existing photos in the databank, the search is a one-to-many search, which means that one probe image is used, and the databank supplies multiple responses.

Facial Recognition Technology and Law Enforcement Use

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.

Masks

The National Institute of Standards and Technology (NIST) has produced reports and continues to study the effect of face masks on the accuracy of FRT. Vendors have

© 2021 Thomson Reuters. All rights reserved. Use of Practical Law websites and services is subject to the Terms of Use (static.legalsolutions.thomsonreuters.com/static/agreement/westlaw-additional-terms.pdf) and Privacy Policy (a.next.westlaw.com/Privacy).

developed new algorithms to address the recognition when a person is wearing a mask and to digitally add masks to the database used.

Some systems use thermal technology to identify people even when part of the face is obscured, for example, from a mask, makeup, glasses, or something else.

Bias

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.)

In addition to the effect of the algorithm on the performance of FRT, other factors include:

- The quality of the probe photo.
- The size of the database used.

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.

Local Government Responses

Some local governments are using the technology and some local governments are not. A few local governments have passed ordinances prohibiting use of FRT (see Oakland, California's ordinance).

Iris Recognition and Retina Scans

Iris recognition involves the use of an automated system that identifies the pigmentated portion of the eye, which has certain unique patterns. Usually, iris recognition requires that the subject be within a few feet from the equipment captured the image of the eye.

Retina scans use equipment which examines the blood vessels in the retina. Retina scans require that the subject 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)).

Handwriting Samples

A handwriting sample may become part of the evidence presented when a handwritten note is used in furtherance of a criminal act or to help identify involvement in a matter. Experts testify about similar or unique characteristics between the handwriting sample and the handwriting recovered as part of a criminal act. The jury decides whether the sample and the other writing are a match. (*United States v. Crisp*, 324 F.3d 261 (4th Cir. 2003).)

A handwriting example is an "identifying physical characteristic" outside the protection of the Fifth Amendment, as the example is not testimonial or communicative (*Gilbert v. California*, 388 U.S. 263 (1967)).

Law Enforcement Use

Police departments have used biometrics, particularly fingerprints for many years. However, some people are uncomfortable with certain newer biometric technologies.

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. Although the cases in this Practice Note address claims against the use of biometric evidence at criminal or civil trials, 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) and see Practice Note, Section 1983: Overview: Actions by Prisoners.)

The 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

© 2021 Thomson Reuters. All rights reserved. Use of Practical Law websites and services is subject to the Terms of Use (static.legalsolutions.thomsonreuters.com/static/agreement/westlaw-additional-terms.pdf) and Privacy Policy (a.next.westlaw.com/Privacy).

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. 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. "Furthermore, the highly technical algorithms which form the heart of Recovery's reports do not lend themselves to critical review through the evaluative techniques available to the average civil litigant." (*Ray v. Recovery Healthcare*, 2021 WL 1102081 (N.D. Tex. March 22, 2021).)

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.

Potential Claims

Depending on the type of biometric process, issues include:

- Constitutional challenges, such as challenges based on:
  - 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; and
  - Sixth Amendment claims that the introduction of biometric evidence violates defendants' right to confront the witnesses against them.
- Hearsay (a claim that the biometric identifier is an out-of-court declaration being offered at trial as proof of the facts asserted). Hearsay claims can overlap with Sixth Amendment claims.
- Privacy (a claim that acquiring or using biometric identifiers violates criminal defendants' or other potential plaintiff's privacy rights). Privacy claims can overlap with the constitutional challenges.
- Reliability, usually based on Federal Rule of Evidence 702 (FRE 702 and see *Daubert*, 509 U.S. 579, 597). The reliability factors a court considers include:
  - whether the technique or theory can be tested (objectively verifiable);
  - whether the technique or theory has been subjected to peer review and publication;
  - error rate for the technique or theory when applied;
  - the standards and controls and the maintenance of those standards;
  - whether the technique or theory has been generally accepted in the scientific community;
  - the relationship of the theory or technique to established reliable techniques;
  - the qualifications of the testifying expert; and
  - nonjudicial use of the technique, that is, whether the technique is used and relied on outside of the courtroom.

(See the see 2000 Advisory Committee Notes to FRE 702.)

For more information about evidence in federal court, see Practice Note, Evidence in Federal Court: Overview.

Hearsay, Privacy, and Constitutional Cases Involving Biometrics

Fourth Amendment Objections to Fingerprints

The Fourth Amendment does not prohibit fingerprinting a person. However, police officers cannot detain someone just to take their fingerprints without a warrant, probable cause, or an applicable exception. This action violates the Fourth Amendment. (*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)).

Fifth Amendment Objections to Fingerprints

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 for the biometric purpose of unlocking a cell phone, court

© 2021 Thomson Reuters. All rights reserved. Use of Practical Law websites and services is subject to the Terms of Use (static.legalsolutions.thomsonreuters.com/static/agreement/westlaw-additional-terms.pdf) and Privacy Policy (a.next.westlaw.com/Privacy).

decisions have been mixed, holding that a fingerprint in that case:

- 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)).

Sixth Amendment and Hearsay Objections to Fingerprints

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).)

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)).

Fourth Amendment Objections to DNA

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 Objections to DNA

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 Objections to DNA

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)).

Facial Recognition Technology and Fourth, Fifth, and Sixth Amendment Objections

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 *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)).

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)). In that case, the court allowed the use of biometrics, but suppressed the defendant's statement about the defendant's passcode as violating the Sixth Amendment right to counsel.

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).)

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)).

© 2021 Thomson Reuters. All rights reserved. Use of Practical Law websites and services is subject to the Terms of Use (static.legalsolutions.thomsonreuters.com/static/agreement/westlaw-additional-terms.pdf) and Privacy Policy (a.next.westlaw.com/Privacy).

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 Standards and Biometrics

Use of biometric identifiers is often challenged based on reliability.

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.

(*Daubert*, 509 U.S. 579 (1993).)

In addition to court cases assessing the reliability of biometric evidence, the National Institute of Standards and Technology (NIST) provides standards itself and also partners with the American National Standards Institute (ANSI) to provide standards as part of work at the Information Technology Laboratory (ANSI/NIST-ITL).

Reliability Standard 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, see Standard for Excluding Expert Testimony: 50 State Survey.

Reliability of Fingerprints

Courts generally have found the *Daubert* factors sufficiently established to support admission of testimony concerning fingerprints (*United States v. Mitchell*, 365 F.3d 215 (3d Cir. 2004)).

The ANSI/NIST-ITL provides fingerprint standards.

Reliability of DNA

Courts have found short tandem repeats (STR) DNA tests to be reliable (*United States v. McCluskey*, 954 F. Supp. 2d 1224 (D.N.M. 2013)).

Reliability of Facial Recognition Technology

Facial recognition technology is an evolving technology. 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 (see Bias).

Facial recognition technology is used to generate leads and not for a final identification or to support other evidence (see Facial Recognition Technology and Law Enforcement Use). Due to its limited role, the prosecution may not offer FRT as evidence, so there may not be a ruling on its admissibility.

Reliability of Iris Scans

A court found iris scans more reliable than fingerprints, but it does not discuss *Daubert* factors. "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).) The case notes that iris scans are used in New York to prevent release of the wrong prisoners and the program is successful in preventing those mistakes.

Reliability of Voice Recognition

Aural spectrographic voice identification is not considered reliable under *Daubert* (see *United States v. Mills*, 2021 WL 2351114 (3d Cir. June 9, 2021)).

Reliability of Handwriting Samples

Courts have found "handwriting comparison testimony has a long history of admissibility in the courts of this

© 2021 Thomson Reuters. All rights reserved. Use of Practical Law websites and services is subject to the Terms of Use (static.legalsolutions.thomsonreuters.com/static/agreement/westlaw-additional-terms.pdf) and Privacy Policy (a.next.westlaw.com/Privacy).

country (see, for example, *Robinson v. Mandell*, 20 F. Cas. 1027 (D.Mass.1868) and *United States v. Crisp*, 324 F.3d 261 (4th Cir. 2003)).

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 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).)

Employment Issues

In addition to public safety, local governments may want to use biometric identifiers for employment purposes. 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).

For additional information on biometrics in the workplace, see Practice Note, Biometrics in the Workplace.

Potential Causes of Action

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

- Genetic Information Nondiscrimination Act (GINA).
- Religious discrimination.
- Age discrimination.
- Stored Communications Act.
- Electronic Communications Privacy.
- State law claims, including unlawful acquisition or retention of biometric identifiers or improper destruction.

Cause of Action Under GINA

The Genetic Information Nondiscrimination Act (42 U.S.C. §§ 2000ff-11) prohibits employers from discriminating based on an employee's genetic information (42 U.S.C. § 2000ff-1). 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.

Genetic Information Nondiscrimination Act claims are often filed together with Americans with Disabilities Claims, age discrimination claims, and claims for retaliation.

Exceptions to GINA include:

- Accidental acquisition of genetic information.
- Receipt of information in a wellness program where the employee voluntarily gives the information,the information is only available for the wellness program, and no individual information is disclosed to the employer. The employer may receive aggregate information.
- 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.

Cause of Action for Religious Discrimination

If an employee's sincerely held religious belief conflicts with the acquisition or use of personal biometric data, the local government employer should explore alternatives to acquisition or use.

In one case, a city instituted new security procedures, including new security cards. The cards required

© 2021 Thomson Reuters. All rights reserved. Use of Practical Law websites and services is subject to the Terms of Use (static.legalsolutions.thomsonreuters.com/static/agreement/westlaw-additional-terms.pdf) and Privacy Policy (a.next.westlaw.com/Privacy).

an employee to be fingerprinted and one employee complained that that process was forbidden by the employee's religious belief, as the employee believed 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).)

Cause of Action for 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. In that case, an employer should consider offering alternative means of access.

Cause of Action Under Stored Communications Act

At this time, courts have not found use of keystrokes or keylogger programs to be a violation of the Stored Communications Act. (*Langston v. Langston*, 2011 WL 4007338 (E.D. Tex. August 31, 2011).)

Cause of Action Under Electronics Communications Privacy

Courts have reached varying decisions about whether monitoring keystrokes violates the Electronics Privacy Act. For example, in *United States v. Scarfo*, the court found that keystrokes were not covered by the Act (180 F. Supp. 2d 572 (D.N.J. 2001)). In *Brahmana v. Lembo*, the court found that keystrokes may be covered (2009 WL 1424438 (N.D. Cal. May 20, 2009)).

Cause of Action Under State Law

The types of actions a plaintiff may bring in relation to acquisition, misuse, retention, or improper destruction of biometric identifiers is currently evolving. 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 (see State Laws).

Plaintiffs may generally allege:

- 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.

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. "The Defendants and other persons at the premises are hereby ordered by the Court to provide any usernames, passwords, login credentials, biometrics (fingerprints, retina scans, or the like) or other information necessary for the technical expert to access Defendants' digital files, computers, folders, and networks, including such login information for Defendants' Dropbox, Google, Skype, or other online account(s)" (*Solar Connect, LLC v. Endicott*, 2018 WL 2386066 (D. Utah April 6, 2018)).

Contract 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.

It is always important that a local government not agree to assume a duty to defend or to indemnify other parties to a contract (see Practice Note, Contract Drafting or Review for Local Governments: Local Government Protections), 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 (see State Laws). Agreeing to defend or indemnify a vendor in a contract, even if those

© 2021 Thomson Reuters. All rights reserved. Use of Practical Law websites and services is subject to the Terms of Use (static.legalsolutions.thomsonreuters.com/static/agreement/westlaw-additional-terms.pdf) and Privacy Policy (a.next.westlaw.com/Privacy).

clauses are not valid, creates additional problems for local governments.

Public Records

All states have statutes allowing access to public records (see State Public Records Laws Chart). 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.

State Laws

There are no comprehensive federal laws about the use of biometrics and some states have laws that address the capture, use, storage, and destruction of biometrics. Other states have not passed legislation addressing this issue. The state laws usually just regulate commercial uses and do not directly affect local government. Examples of state laws include:

Illinois

The first state to address this issue was Illinois in 2008. The Illinois law:

- Applies to private entities. It does not apply to local or governmental entities.
- Requires the entity to give notice and get a written release before obtaining biometric information.
- Forbids disclosure (with some exceptions) and does not allow an entity to sell or profit form someone else's biometric information.
- Requires a retention schedule.
- Provides for a cause of action and liquidated damages.

(740 ILCS 14/1 to 14/99.)

For more information on limitations and acceptable uses of biometric information by Illinois employers, see Practice Note, Biometrics in the Workplace.

Texas

The Texas law:

- Prohibits possession for commercial purposes.
- Does not allow a person to sell, lease, or disclose identifiers, with some exceptions. One exception is disclosure to a law enforcement agency in response to a warrant.
- Requires protection from disclosure.
- Requires destruction after one year, unless legally required to keep it longer.
- Provides for a civil penalty.

(Tex. Bus. & Com. Code Ann. § 503.001.)

For more information on limitations and acceptable uses of biometric information by Texas employers, see Practice Note, Biometrics in the Workplace; State Q&A, Employee Privacy Laws: Texas: Biometric Identifiers: Tex. Bus. & Com. Code Ann. § 503.001.

California

California's law does not include local governments directly. The law regulates collection of personal information, which includes biometric information (Cal. Civ. Code § 1798.140). Provisions of the law include requirements to:

- Inform people about personal information collected (Cal. Civ. Code § 1798.100).
- Delete the information when requested (with some exceptions) (Cal. Civ. Code § 1798.105).
- Disclose information to consumer when requested to do so (Cal. Civ. Code §§ 1798.110, 1798.115).
- Allow the consumer to opt-out of the sale of their information (Cal. Civ. Code § 1798.120).
- Prohibit a business from discrimination because a consumer exercised options under the state law (Cal. Civ. Code § 1798.125).

(Cal. Civ. Code § 1798.100-1798.199.95.)

For more information on limitations and acceptable uses of biometric information by California employers, see State Q&A, Employee Privacy Laws: California: Searches, Surveillance, and Biometric Information; Practice Note, California Consumer Privacy Act's (CCPA) Impact on Employers: Overview.

Colorado

Colorado's law concerns personal information, but personal information includes biometric information.

© 2021 Thomson Reuters. All rights reserved. Use of Practical Law websites and services is subject to the Terms of Use (static.legalsolutions.thomsonreuters.com/static/agreement/westlaw-additional-terms.pdf) and Privacy Policy (a.next.westlaw.com/Privacy).

A covered entity must have a policy for destroying personal information collected (Colo. Rev. Stat. Ann. § 6-1-713).

The definition for covered entity includes a person maintaining, owning, or licensing personal identifying information in the course of their business. A person is defined as including a legal entity (Colo. Rev. Stat. Ann. § 6-1-102). The definition does not expressly exclude a governmental entity.

For more information on limitations and acceptable uses of biometric information by Colorado employers, see State Q&A, Employee Privacy Laws: Colorado: Searches, Surveillance, and Biometric Information.

Iowa

Iowa requires notification of a security breach of computerized data that includes personal information (Iowa Code Ann. § 715C.2). Personal information includes biometric data (Iowa Code Ann § 715C.1).

Although the law requires a person to notify a consumer if the consumer's personal information was breached, the law appears to affect local government because the definition of person includes local government (Iowa Code Ann. § 715C.1).

Consumer is defined to mean an individual who is a resident of the state (Iowa Code Ann. § 715C.1).

For more information on limitations and acceptable uses of biometric information by Iowa employers, see State Q&A, Employee Privacy Laws: Iowa: Searches, Surveillance, and Biometric Information.

Washington

Washington's law applies to commercial uses (RCW 19.375.010) and does not apply to law enforcement activities (RCW 19.375.040). The Washington law requires:

- Notice and consent before enrolling a biometric identifier (with some exceptions).
- Safeguards in storage of biometric identifiers.
- Retention for no longer than is necessary.

(RCW 19.375.010.)

For more information on limitations and acceptable uses of biometric information by Washington employers, see State Q&A, Employee Privacy Laws: Washington: Searches, Surveillance, and Biometric Information; Practice Note, Biometrics in the Workplace.

Maryland

There are several statutes concerning biometrics in Maryland.

Laws Applicable to Local Government

A unit (defined to include a city or county, see Md. Code Ann., State Gov't § 10-1301) must:

- Prevent unauthorized access of personal information (which includes biometric identifiers) during record destruction (Md. Code Ann., State Gov't § 10-1303).
- Have reasonable security procedures (Md. Code Ann., State Gov't § 10-1304).
- Investigate if a security breach occurs (Md. Code Ann., State Gov't § 10-1305).
- Notify an affected individual if a security breach occurs (with some exceptions) (Md. Code Ann., State Gov't § 10-1305).
- If the unit has to give notice to more than 1,000 people, then the unit must also notify consumer reporting agencies (Md. Code Ann., State Gov't § 10-1307).

Other Maryland Laws

An employer cannot create a facial template of an applicant during an employment interview, unless the applicant signs a waiver (Md. Code Ann., Lab. & Empl. § 3-717). When a business is destroying personal information of an employee, a former employee, or a customer, including biometric information, it must prevent unauthorized access or use of that information (Md. Code Ann., Com. Law § 14-3502).

For more information on limitations and acceptable use of biometric information by Maryland employers, see State Q&A, Employee Privacy Laws: Maryland: Facial Recognition Technology for Applicants: Md. Code Ann., Lab. & Empl. § 3-717; State Q&A, Employee Privacy Laws: Maryland: Biometric Information.

Massachusetts

The use of biometric information is likely analyzed under the Massachusetts Privacy Act (M.G.L. c. 214, § 1B). For more information on limitations and acceptable uses of biometric information by Massachusetts employers, see State Q&A, Employee Privacy Laws: Massachusetts: Biometric Information.

© 2021 Thomson Reuters. All rights reserved. Use of Practical Law websites and services is subject to the Terms of Use (static.legalsolutions.thomsonreuters.com/static/agreement/westlaw-additional-terms.pdf) and Privacy Policy (a.next.westlaw.com/Privacy).

New York

New York prohibits employers from fingerprinting employees, but state and municipal employees are excepted (N.Y. Lab. Law § 201-a). For more information on the limitations and acceptable use of biometric information by New York employers, see State Q&A, Employee Privacy Laws: New York: Biometric Information.

Vermont

Vermont has addressed biometric identifiers under its data broker laws (see Article, Trends in Privacy and Data Security: 2020: Biometrics Privacy).

About Practical Law

Practical Law provides legal know-how that gives lawyers a better starting point. Our expert team of attorney editors creates and maintains thousands of up-to-date, practical resources across all major practice areas. We go beyond primary law and traditional legal research to give you the resources needed to practice more efficiently, improve client service and add more value.

If you are not currently a subscriber, we invite you to take a trial of our online services at legalsolutions.com/practical-law. For more information or to schedule training, call 1-800-733-2889 or e-mail referenceattorneys@tr.com.

THOMSON REUTERS®