Biometric Laws FAQs

1. What is biometric information?

Definitions vary by state, but in general, biometric information refers to unique biometric identifiers such as fingerprints, facial patterns or scans, voice patterns, and iris recognition.

2. How are companies collecting biometric information?

Biometric information is increasingly collected and used by businesses for many reasons, including payment authentication, security screening, timekeeping systems, and fraud detection.

3. How common are biometric privacy laws?

Laws regulating biometric information are gradually being enacted by the states:

- Three states have passed biometric privacy laws that directly regulate collection, use, disclosure, and destruction of biometric information: Illinois, Texas, and Washington.[1]
- Nineteen states have incorporated biometric data into their definition of "Personal Information," requiring notification to affected individuals in the case of a data breach.[2]
- As discussed below, five states have enacted laws that, while not explicitly introduced as biometric privacy laws, regulate biometric information in some way: **California**, **Colorado**, **New York**, **North Carolina**, and **Florida**. See question 6 for details on the laws enacted by each state.
- Municipalities are also starting to pass biometric related laws, such as San Francisco, Oakland, and Somerville's facial-recognition ban.

4. How do biometric privacy laws work?

Biometric privacy law varies from state to state and city to city; however, the laws all generally require some form of notice and consent before the biometric information is collected from an individual. Illinois also requires a "written policy" to be made publicly available with specific requirements as to its content. Sale, lease, or disclosure of biometric information to third parties is generally prohibited unless the individual consents or an exception applies.[3]

Each biometric privacy law requires that the biometric information be destroyed when it is no longer needed for the purpose for which it was collected, subject to applicable legal requirements that may mandate a longer retention period. Some states specify when data must be destroyed. For example, Texas requires that data be destroyed within a reasonable time, but not later than the first anniversary of the date when the purpose for the collecting expires, unless another law provides for a longer maintenance period.

5. What are the potential penalties/risks for violating biometric privacy laws?

The remedies available for violations of biometric privacy laws are different in each state. In Texas, the only available remedy is for the attorney general to seek a civil penalty for up to $25,000 per violation. In Illinois, however, any "aggrieved" person can file suit for either liquidated or actual damages, attorneys' fees, and injunctive relief. Class actions are also permitted. After the Illinois Supreme Court's recent decision in *Rosenbach v. Six Flags Entertainment Corp.*, an Illinois plaintiff no longer needs to show he or she was injured from the violation, opening companies up to the potential for large class actions for liquidated damages and attorneys' fees.[4]

[1] Ten additional states have proposed biometric privacy legislation that has not yet been enacted: Alaska, Arizona, Connecticut, Delaware, Florida, Indiana, Massachusetts, Michigan, Montana, New Hampshire, and New York. Many of these bills failed or died in committee, but it is likely that legislators will continue to be active in this area going forward.
[2] Those states are: Arizona, California, Colorado, Delaware, Florida, Illinois, Iowa, Louisiana, Maryland, Missouri, Nebraska, New Mexico, North Dakota, North Carolina, Oregon, South Dakota, Texas, Wisconsin and Wyoming.
[3] For example, the laws generally permit disclosure to complete a financial transaction authorized by the individual and in cases where the disclosure is required by law. Texas law permits disclosure for identification purposes in the event of the individual's disappearance or death.
[4] Rosenbach v. Six Flags Entertainment Corp., No. 123186, 2019 IL 123186 (Jan. 25, 2019).

Frost Brown Todd LLC
ATTORNEYS

6. What other states have laws with restrictions relating to biometric information?

CALIFORNIA	California labor law makes it a misdemeanor for an employer to require an employee to be fingerprinted as a condition of employment if the employer plans to provide the information to a third party and if the information could be used to the employee's detriment.[5]
NEW YORK	New York labor law prohibits employers from fingerprinting employees as a condition of employment or continued employment unless specifically authorized by another law.[6] On April 22, 2010, the New York Department of Labor issued an opinion clarifying that if a finger print is captured, even if it is not stored, it is prohibited under the law.[7] Voluntary fingerprinting of employees is not prohibited under this law. However, employees cannot be coerced into volunteering. **In short, a time clock that captures fingerprints should not be used in New York unless the employee volunteers to use the system.**
COLORADO	Colorado requires employers to develop policies to properly secure and dispose of paper and electronic documents containing "personal identifying information," which is defined to include biometric information.[8]
NORTH CAROLINA	North Carolina includes biometric data, when attached to a person's name, as personal information for purposes of its Identity Theft Protection Act.[9] Entities that have such information must take reasonable measures to protect against unauthorized access to this information. In addition, North Carolina requires development and implementation of policies relating to proper disposal of this information.
FLORIDA	Florida bars public schools from collecting, obtaining or retaining any biometric information from their students or their immediate family members.[10]

7. What are some best practices regarding biometric data?

The landscape regarding biometrics laws is changing rapidly and varies from jurisdiction to jurisdiction. While there is not a one-size-fits-all approach, there are several best practices that you can follow when collecting biometric data.

- ☑ Provide notice before collecting, using, or disclosing biometric information. That notice should include information about the data that is being collected, what it will be used for, who it will be shared with and for what purpose, and how long it will be stored.
- ☑ Obtain consent before collecting biometric information.
- ☑ Use, share, and disclose biometric information only as set forth in your biometric notice.
- ☑ Store biometric information securely and only for as long as needed.
- ☑ Develop policies and procedures to securely destroy biometric information when it is no longer needed.
- ☑ If you have a data breach, consider whether a breach of biometric information should be reported under applicable laws.
- ☑ Consult your attorneys before collecting biometric information from your employees or other individuals, as this area of law is rapidly developing.

For more information about biometric laws, contact Frost Brown Todd's Privacy & Data Security Team:

Melissa Kern
Member and Team Co-chair
mkern@fbtlaw.com
513.651.6898

Victoria Beckman
Member and Team Co-chair
vbeckman@fbtlaw.com
614.559.7285

Zachary Hoyt
Associate
zhoyt@fbtlaw.com
502.779.8625

[5] Cal. Lab. Code § 1051.
[6] N.Y. Lab. Law § 201-a.
[7] The opinion is available here. Instruments that measure the geometry of the hand are permissible under the labor law so long as they do not scan the surface details of the hand and fingers in a manner similar to scanning of a fingerprint. *Id.*
[8] Colo. Rev. Stat. Ann. § 6-1-713(1), (2).
[9] N.C.G.S. 75-61, 65.
[10] Fla. Stat. § 1002.222(1)(a).