Biometric Privacy: Mitigating Legal Risks When Using Biometric Technologies

Maintained

by *David J. Oberly*, Squire Patton Boggs LLP

This practice note discusses the legal issues regarding biometric data. Specifically, this note covers the major types of biometric technologies, state and local laws governing the collection and use of biometric data, Federal Trade Commission enforcement, and how to mitigate legal risks when using biometric technologies in commercial operations. To get ahead of the compliance curve, companies must take proactive measures to establish adaptable biometric privacy compliance programs. Doing so will facilitate compliance with current biometric privacy laws and allow businesses to adeptly respond to the ever-expanding web of biometric privacy laws.

For more information regarding biometric privacy compliance, see *Biometric Privacy State Law Survey*, *Biometrics Workplace Compliance and Best Practices for Employers*, and *Biometric Privacy Compliance Checklist*.

What Is Biometric Data?

"Biometrics" are measurable human biological characteristics and behavior that are used to identify and authenticate individuals' identities, and the automated methods of recognizing or analyzing a person based on those characteristics. "Biometric data" encompasses data derived from automatic measurements of those biological characteristics and behavior.

U.S. biometric privacy laws refer to biometric data as "biometric identifiers" and "biometric information." Biometric identifier includes a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric information is a catchall term that encompasses any information based on an individual's biometric identifier that is used to identify an individual.

Biometric data offers a range of noteworthy benefits to companies across all industries, including:

- Convenience
- Security/access control
- Fraud reduction -and-
- Cost savings

At the same time, biometric data also presents a unique set of risks and challenges, particularly in the areas of privacy, security, and discrimination/bias. Today, the question is not whether companies should use biometric data, but how they can leverage its benefits in a way that minimizes legal and reputational risks.

As explained in more detail below, the biometric privacy legal landscape is uncertain and evolving. At this time, there is no comprehensive federal biometric privacy regulatory regime that governs the collection and use of biometric data; consequently, companies and their counsel must navigate an increasing patchwork of differing laws and their potential application to specific uses of biometric data.

Major Types of Biometric Technologies

Today, the most widely used types of biometric technologies are facial recognition, voice biometrics (voiceprints), and fingerprint biometrics.

Facial Recognition

Facial recognition technology involves the process of using biometrics to scan or digitally map an individual's facial features or geometry, such as the distance between the eyes or the forehead and chin. These measurements are then used to create a mathematical algorithm or formula known as a "facial template" or "facial signature" of the extracted facial geometry data. An algorithm is then used to compare the extracted facial data with previously generated, stored facial geometry data to identify or verify an individual associated with the extracted facial template.

Voiceprints

Voice biometric technology relies on the analysis of unique voice patterns to identify or verify the identity of individuals. "Voiceprint" is generally defined as a distinctive pattern of curved lines and whorls made by a machine that measures human vocal sounds for the purpose of identifying an individual speaker. It is this hallmark of identifying (or verifying) the identity of an individual that makes voice data a voiceprint under U.S. biometric privacy laws.

Fingerprints

Biometric fingerprint technology involves the process of using biometrics to scan or digitally map an individual's finger geometry-such as its length, width, thickness, and surface area-when placed on a biometric scanner. These measurements are then used to create a digital template of the extracted finger geometry data. An algorithm is then used to compare the extracted data with previously generated, stored finger geometry data to identify or verify an individual associated with the extracted fingerprint data.

Legal Landscape Overview – Methods of Regulating Biometric Data Generally

Due to concerns about companies using biometrics in a safe and responsible manner, lawmakers across the country have sought ways to strictly regulate the collection and use of biometric data. These methods include targeted biometric privacy laws, Federal Trade Commission (FTC) enforcement, consumer privacy laws, and data breach notification laws.

Targeted Biometric Privacy Laws

The most significant way that lawmakers regulate the collection and use of biometric data is through targeted biometric privacy laws.

Currently, there are only three active, broad-based biometric privacy laws that have been enacted in the United States:

- Illinois's Biometric Information Privacy Act (BIPA), *740 Ill. Comp. Stat. Ann. 14/1 et seq.*
- Texas's Capture or Use of Biometric Identifier Act (CUBI), *Tex. Bus. & Com. Code § 503.001* -and-
- Washington's HB 1493 (HB 1493), *Wash. Rev. Code § 19.375.010 et seq.*

More recently, new forms of targeted biometric privacy laws have been enacted in the United States, including blanket bans on private sector use of facial recognition technology and requirements and restrictions placed on the use of biometric data by specific industries or sectors.

Federal Trade Commission Enforcement

The FTC has made policing improper facial recognition practices a main priority for the country's de facto privacy and security regulator at the federal level. By pursuing enforcement actions against companies that engage in "unfair or deceptive acts and practices" under Section 5 of the Federal Trade Commission Act (FTC Act), *15 U.S.C. § 45*, the FTC has significantly enhanced the scope of liability exposure associated with the commercial use of biometric technologies-and facial recognition, in particular.

Consumer Privacy Laws

New state consumer privacy laws also now include biometric data within their definitions of covered personal information.

Data Breach Notification Laws

State legislators have amended their data breach notification laws to add biometric data to the types of personal information which, if compromised, trigger breach notification obligations by impacted entities.

State-Level Laws

Illinois, Texas, and Washington have all enacted broad-based biometric privacy law.

Illinois Biometric Information Privacy Act (BIPA)

Of the three active, targeted biometric privacy laws on the books at this time, Illinois's BIPA, *740 Ill. Comp. Stat. Ann. 14/1 et seq.*, is considered the most stringent and has created the greatest amount of liability exposure for companies that use biometric data in their operations.

Applicability and Scope

BIPA applies to "private entities," which is defined as "any individual, partnership, corporation, limited liability company, association, or other group, however, organized." *740 Ill. Comp. Stat. Ann. 14/10*.

BIPA governs the collection and possession of "biometric identifiers" and "biometric information." Biometric identifier is defined as a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. *740 Ill. Comp. Stat. Ann. 14/10*. Biometric information means any information based on an individual's biometric identifier used to identify an individual. *740 Ill. Comp. Stat. Ann. 14/10*.

Core Compliance Requirements

BIPA is comprised of five core compliance requirements:

- **Privacy policy and data retention/destruction guidelines/schedule.** Companies must implement a publicly available privacy policy which establishes the organization's retention schedule and guidelines for permanently destroying biometric data. *740 Ill. Comp. Stat. Ann. 14/15(a)*. Companies are required to permanently destroy biometric data whenever the first of the following occurs: (1) the initial purpose for collecting and obtaining the biometric data has been satisfied or (2) within three years of the individual's last interaction with the private entity. Id.
- **Written notice.** Before collecting any biometric data, companies must provide written notice to individuals or their legally authorized representatives. At a minimum, this notice must provide:
    - That biometric data is being collected or stored
    - The specific purpose for the collection of biometric data -and-
    - The length of time the biometric data will be collected, stored, and used by the company

  740 Ill. Comp. Stat. Ann. 14/15(b)(1)–(2).

- **Written consent/release.** Companies must obtain written consent-referred to as a "written release" in the text of the statute-from individuals before collecting, capturing, or otherwise obtaining their biometric data. *740 Ill. Comp. Stat. Ann. 14/15(b)(3)*; *740 Ill. Comp. Stat. Ann. 14/10*. Companies must also obtain consent before disclosing biometric data to any third parties. *740 Ill. Comp. Stat. Ann. 14/15(d)*.
- **Data security.** Companies must maintain data security measures to safeguard biometric data from unauthorized access, disclosure, or acquisition using the reasonable standard of care within the private entity's industry and measures that are the same as or more protective than the manner in which the company safeguards other types of confidential and sensitive information. *740 Ill. Comp. Stat. Ann. 14/15(e)*.
- **Prohibition on selling, leasing, trading, or profiting from biometric data.** Lastly, companies are strictly prohibited from selling, leasing, trading, or otherwise profiting from an individual's biometric data. *740 Ill. Comp. Stat. Ann. 14/15(c)*.

Enforcement and Penalties/Damages

BIPA is enforced through a private right of action allowing individuals to pursue class litigation against companies that run afoul of the law. *740 Ill. Comp. Stat. Ann. 14/20*. Any person aggrieved by a BIPA violation can recover for each violation:

- Statutory damages of $1,000 or actual damages, whichever is greater, for negligent violations
- Statutory damages of $5,000 or actual damages, whichever is greater, for intentional or reckless violations
- Attorney's fees and costs, including expert witness fees and other litigation expenses -and-
- Other relief, including an injunction, as the court may deem appropriate

740 Ill. Comp. Stat. Ann. 14/20.

Importantly, in Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186 (Ill. 2019), the Illinois Supreme Court interpreted the term "aggrieved" to mean merely suffering an infringement of a legal right, without more. Consequently, under *Rosenbach*, BIPA plaintiffs are entitled to recover statutory damages whenever a private entity fails to comply with one of BIPA's requirements, even if those violations do not result in any actual harm or injury to the plaintiff.

Texas Capture or Use of Biometric Identifier Act (CUBI)

Following the enactment of BIPA in 2008, a year later Texas passed the current version of its own biometric privacy law, CUBI, *Tex. Bus. & Com. Code § 503.001*.

Applicability and Scope

CUBI applies to the capture or collection of biometric identifiers for commercial purposes.

Biometric identifier is defined as a "retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry." *Tex. Bus. & Com. Code § 503.001(a)*.

"Commercial purpose" is not defined by the statute. In the absence of additional guidance, you should assume that commercial purpose includes the collection and use of biometric data for any business purpose or related purpose tied to organizational operations.

Core Compliance Requirements

CUBI is fairly similar to BIPA in terms of its core requirements, which include the following:

- **Data retention/destruction schedule.** Companies that possess biometric data must destroy that data within a "reasonable time," but no later than one year after the initial purpose for collecting the biometric data has

been satisfied. *Tex. Bus. & Com. Code § 503.001(c-1)*. If biometric data is collected for security purposes by an employer (which is not defined in the text of the statute), the purpose for collection is presumed to expire upon termination of the employment relationship. *Tex. Bus. & Com. Code § 503.001(c-2)*.

- **Notice.** Before capturing any biometric data, companies must provide notice to individuals informing them that biometric data is being collected. Unlike BIPA, however, CUBI does not require that this notice be in writing. *Tex. Bus. & Com. Code § 503.001(b)(1)*.
- **Consent.** Companies must obtain consent from individuals before collecting their biometric data. Similar to the law's notice requirement, CUBI also does not require that consent be obtained in writing. *Tex. Bus. & Com. Code § 503.001(b)(2)*.
- **Data security.** Companies must maintain data security measures to safeguard biometric data from unauthorized access, disclosure, or acquisition using "reasonable care" and measures that are the same as or more protective than the manner in which the company safeguards other types of confidential information. *Tex. Bus. & Com. Code § 503.001(c)(2)*.
- **Limitations on selling, leasing, or disclosing biometric data.** Lastly, companies are prohibited from selling, leasing, or otherwise disclosing biometric data unless one of four narrow exceptions applies: (1) consent is given for the disclosure for identification purposes in the event of the individual's disappearance or death, (2) the disclosure completes a financial transaction, (3) the disclosure is permitted by a federal or state statute, or (4) the disclosure is made to a law enforcement agency in response to a warrant. *Tex. Bus. & Com. Code § 503.001(c)(1)(A)-(D)*.

Enforcement and Penalties/Damages

Unlike BIPA, CUBI does not provide a private right of action for individuals to pursue class action litigation. Rather, enforcement authority over CUBI rests exclusively with the Texas attorney general. Violations of CUBI may subject an entity to civil penalties of up to $25,000 per violation, with no maximum cap. *Tex. Bus. & Com. Code § 503.001(d)*.

Washington HB 1493

In 2017, Washington became the third state to enact a targeted biometric privacy law, HB 1493, *Wash. Rev. Code § 19.375.010 et seq.*

Applicability and Scope

HB 1493 applies to the enrollment of biometric identifiers for a commercial purpose. See *Wash. Rev. Code § 19.375.010 et seq.*

Biometric identifier is defined as "data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual." *Wash. Rev. Code § 19.375.010(1)*. Commercial purpose is defined to mean "a purpose in furtherance of the sale or disclosure to a third party of a biometric identifier for the purpose of marketing of goods or services when such goods are unrelated to the initial transaction in which a person first gains possession of an individual's biometric identifier." *Wash. Rev. Code § 19.375.010(4)*.

Enrollment means when (1) a biometric identifier is captured; (2) converted into a reference template, such as a fingerprint template; and (3) subsequently stored in a database that matches the biometric identifier to a specific individual. *Wash. Rev. Code § 19.375.010(5)*.

Core Compliance Requirements

HB 1493's compliance requirements are similar to BIPA and CUBI in certain respects, but depart significantly from the Illinois and Texas laws in others:

- **Data retention/destruction.** Companies who enroll and thereafter possess biometric data may retain that data no longer than is necessary to provide the services for which the biometric identifier was enrolled. However, biometric data may be held for a longer period of time where it is reasonably necessary to either:
    - ○ Comply with a court order, statute, or public records retention schedule specified by law -or-
    - ○ Protect against or prevent actual or potential fraud, criminal activity, claims, security threats, or liability

  Wash. Rev. Code § 19.375.020(4)(b).
- **Notice.** Before enrolling any biometric data for a commercial purpose, companies must provide notice, which the law defines as "a disclosure, that is not considered affirmative consent, that is given through a procedure reasonably designed to be readily available to affected individuals." *Wash. Rev. Code § 19.375.020(1)*. Under HB 1493, "[t]he exact notice and type of consent required to achieve compliance . . . is context-dependent." *Wash. Rev. Code § 19.375.020(2)*.
- **Consent.** Before enrolling any biometric data for a commercial purpose, companies must also obtain consent for the use of such data. *Wash. Rev. Code § 19.375.020(1)*. In addition, before using or disclosing biometric data in a manner that is materially inconsistent with the terms under which the data was originally provided, consent must be obtained for the new terms of use or disclosure. *Wash. Rev. Code § 19.375.020(5)*.
- **Limitations on selling, leasing, or disclosing biometric data.** Unless consent is obtained from the individual, a company may not sell, lease, or otherwise disclose that individual's biometric data unless the disclosure is:
    - ○ Necessary to provide a product or service subscribed to, requested, or expressly authorized by the individual
    - ○ Necessary to facilitate or complete a financial transaction (and any third party to whom the biometric data is disclosed maintains the confidentiality of the data and does not further disclose the data unless otherwise permitted under the law)
    - ○ Required or expressly authorized by federal statute, state statute, or court order
    - ○ Made to a third party who contractually promises that the biometric data will not be further disclosed and will not be used for a purpose that is inconsistent with the notice- and consent-related terms under which the biometric data was originally submitted -or-
    - ○ Made to prepare for litigation or to respond to or participate in the judicial process

  Wash. Rev. Code § 19.375.020(3).
- **Data security.** Lastly, companies must maintain data security measures to safeguard biometric data using reasonable care to guard against unauthorized access and acquisition. *Wash. Rev. Code § 19.375.020(4)(a)*.

Enforcement and Penalties/Damages

Like CUBI, HB 1493 lacks a private right of action provision. Rather, the power to enforce the law rests exclusively with the state's attorney general under the state's consumer protection act. Violations of HB 1493 may subject a company to civil penalties of up to $2,000 per violation. *Wash. Rev. Code § 19.375.030*.

Municipal-Level Laws

New York City (New York), Portland (Oregon), and Baltimore (Maryland) have all enacted some form of biometric privacy law.

New York City "Commercial Establishments" Biometric Identifier Information Ordinance

In mid-2021, the New York City Council enacted the nation's first municipal-level biometric privacy law regulating commercial establishments (the NYC Biometrics Ordinance), *N.Y.C. Admin. Code § 22-1201 et seq.*, which went into effect in July 2021.

Scope and Applicability

The NYC Biometrics Ordinance applies to "commercial establishments," which is defined broadly to mean "a place of entertainment, a retail store, or a food and drink establishment." *N.Y.C. Admin. Code § 22-1201*.

The NYC Biometrics Ordinance applies to the collection and use of "biometric identifier information," which is also defined broadly as any "physiological or biological characteristic that is used by or on behalf of a commercial establishment, singly or in combination, to identify, or assist in identifying, an individual, including but not limited to: (i) a retina or iris scan, (ii) a fingerprint or voiceprint, (iii) a scan of hand or face geometry, or any other identifying characteristic." *N.Y.C. Admin. Code § 22-1201*.

Core Compliance Requirements

Unlike state-level biometric privacy laws, the NYC Biometrics Ordinance is much narrower in scope-and is comprised of two main compliance requirements:

- **Notice.** Commercial establishments must provide notice by posting clear and conspicuous signage near all customer entrances. N.Y.C. Admin. § 22-1202(a).
- **Prohibition on sharing, trading, leasing, selling, or otherwise profiting from biometric data transactions.** Commercial establishments are strictly prohibited from sharing in exchange for anything of value, trading, leasing, selling, or otherwise profiting from any transaction involving biometric data. N.Y.C. Admin. § 22-1202(b).

Enforcement and Damages/Penalties

The NYC Biometrics Ordinance is enforced through a private right of action. See N.Y.C. Admin. § 22-1203. Any person "aggrieved" by a violation of the ordinance can recover (1) statutory damages of $500 per each violation of the ordinance's notice requirement; (2) statutory damages of $500 per each negligent violation of the ordinance's ban on selling or profiting from biometric data; (3) statutory damages of $5,000 per each intentional or reckless violation of the ban on selling or profiting from biometric data; (4) reasonable attorney's fees and costs, including expert witness fees and other litigation expenses; and (5) "other relief," including an injunction, as the court may deem appropriate. N.Y.C. Admin. § 22-1203.

The NYC Biometrics Ordinance also contains a written notice and cure period requirement that requires commercial establishments to be given notice of any purported violations of the law's notice requirement at least 30 days before litigation can be commenced. N.Y.C. Admin. § 22-1203. If the establishment cures the violation and provides a written statement that the violation has been cured and no further violations will occur within the 30-day period, no legal action can be pursued in connection with the alleged violations. N.Y.C. Admin. § 22-1203.

New York City Tenant Data Privacy Act (TDPA)

Shortly after passing the NYC Biometric Ordinance, New York City added to the growing web of biometric privacy regulation with its enactment of the Tenant Data Privacy Act (TDPA), *N.Y.C. Admin. Code § 26-3001 et seq.*, which regulates the biometric data practices of owners and operators of "smart access buildings" located in New York City.

Companies that implement smart access systems after the law's July 29, 2021, effective date must comply immediately with the ordinance. N.Y.C. Int. No. 1760-A, app A § 2. However, companies that already had smart access systems in place as of the effective date of the ordinance are given until January 1, 2023, to comply. This allows owners to replace or upgrade their smart access systems to comply with the law. N.Y.C. Int. No. 1760-A, app A § 2.

Applicability and Scope

The TDPA applies to owners of smart access buildings that utilize "smart access systems." A smart access building includes any type of home or other residence that is rented by three or more families. N.Y.C. Admin. § 26-3001. A smart access system is one that uses any type of digital technology-including biometric identifier information-to grant entry to a smart access building, including its common areas or individual dwelling units. N.Y.C. Admin. § 26-3001.

The TDPA governs the collection and use of biometric identifier information, which is defined as a physiological, biological, or behavioral characteristic that is used to identify, or assist in identifying, an individual, including:

- A retina or iris scan
- A fingerprint
- A voiceprint
- A scan or record of a palm, hand, or face geometry
- Gait or movement patterns -or-
- Any other similar identifying characteristic

N.Y.C. Admin. § 26-3001.

Two other definitions of importance to the TDPA are "reference data" and "authentication data." Reference data refers to data that is initially collected to be used by a smart access system to verify an individual's identity. N.Y.C. Admin. § 26-3001. Authentication data refers to data that is generated or collected at the point of authentication-in other words, at the time an individual seeks access to a building. N.Y.C. Admin. § 26-3001.

Compliance Requirements

Under the TDPA, owners of smart buildings that regulate access with the help of biometrics must adhere to the following requirements and limitations:

- **Data collection limitations.** Owners may collect biometric data only if its smart access system utilizes such information. N.Y.C. Admin. § 26-3002(a). In addition, even when collection is permitted, owners are barred from collecting any additional biometric data beyond which is needed to operate its smart access system. N.Y.C. Admin. § 26-3002(a).
- **Express consent.** Before any biometric data is collected, tenants and guests must first provide their express consent, either in writing or through a mobile application. N.Y.C. Admin. § 26-3003(a)(6).
- **Privacy policies.** Owners must provide tenants with a written privacy policy that contains specific information about the owner's biometric access system, including a description of what type(s) of biometric data are collected, how the data is secured, and how long the data is retained before it is destroyed. N.Y.C. Admin. § 26-3004.
- **Retention limitations.** Subject to certain limited exceptions, biometric data must be permanently destroyed within specified time frames; namely, 90 days after authentication data is collected and 90 days after a tenant moves out or a visitor's access expires. N.Y.C. Admin. § 26-3002(b)-(d).
- **Prohibition on other uses of biometric data.** Biometric data cannot be sold, leased, or disclosed unless a tenant or visitor gives express authorization in writing or through a mobile application (or one of several other narrow exemptions applies). N.Y.C. Admin. § 26-3003(a)(1).
- **Security measures.** "Stringent" security measures must be maintained to safeguard biometric data, including-at a minimum-encryption, firmware that allows for the remediation of any security or vulnerability issues, and the ability to change passwords (if they are used). N.Y.C. Admin. § 26-3005.

Enforcement and Damages/Penalties

The TDPA is enforced through a limited private right of action that allows individuals to bring claims for alleged unlawful sales of biometric data. N.Y.C. Admin. § 26-3005. Individuals can recover the following damages for the unlawful sale of data:

- For each occupant and each unlawful sale:
    - Compensatory damages and, in the court's discretion, punitive damages -or-
    - At the election of each occupant, damages ranging from $200 to $1,000
- Reasonable attorney's fees and court costs -or-
- Any other relief the court determines to be appropriate

N.Y.C. Admin. § 26-3005.

Private Sector Facial Recognition Bans

Portland, Oregon

In September 2020, a new type of biometric privacy regulation was added to the legal landscape: outright private sector bans on the use of certain types of biometric technologies. The city of Portland, Oregon became the first jurisdiction to enact a sweeping, across-the-board ban prohibiting the use of facial recognition software by private entities (the Portland FRT Ordinance), Portland, Or., City Code Ch. 34.10, which went into effect at the start of 2021.

Applicability and Scope

The Portland FRT Ordinance applies to the use of "face recognition technologies" by private entities. "Private entity" is defined in a very similar fashion to BIPA as "any individual, sole proprietorship, partnership, limited liability company, association, or any other legal entity, however organized." PCC § 34.10.020(E).

Face recognition technologies means "automated or semi-automated processes using face recognition that assist in identifying, verifying, detecting, or characterizing facial features of an individual or capturing information about an individual based on an individual's face." PCC § 34.10.020(B). Face recognition, in turn, is defined as "the automated searching for a reference image in an image repository by comparing the facial features of a probe image with the features of images contained in an image repository (one-to-many-search)." PCC § 34.10.020(A).

Core Compliance Requirement

Under the Portland FRT Ordinance, private entities are barred from using face recognition technologies in any "places of public accommodation"-defined as "[a]ny place or service offering to the public accommodations, advantages, facilities, or privileges whether in the nature of goods, services, lodgings, amusements, transportation, or otherwise"-within the boundaries of the city of Portland. PCC § 34.10.030; PCC § 34.10.020(D).

Enforcement and Penalties/Damages

The Portland FRT Ordinance is enforced by a private right of action. PCC § 34.10.050. Any person "injured by a material violation" of the ordinance can recover (1) actual damages or statutory damages of $1,000 per day for each day of violation, whichever is greater and (2) any other remedies "as may be appropriate." PCC § 34.10.050.

Baltimore, Maryland

In July 2021, Baltimore became the second U.S. jurisdiction to enact an outright private sector ban on the use of facial biometrics (the Baltimore FRT Ordinance), Baltimore, Md., City Code Art. 19, subt. 18. In so doing, Baltimore pushed the boundaries of its regulation even further than Portland by imposing criminal penalties for noncompliance.

Scope and Applicability

The Baltimore FRT Ordinance applies to the use of "face surveillance systems" by persons. "Persons" is defined as "an individual, partnership, firm, association, corporation, or other entity of any kind." Balt. Code, Police § 18-1(e).

Face surveillance system means "any computer software or application that performs face surveillance." Balt. Code, Police § 18-1(c)(1). Face surveillance, in turn, means "an automated or semi-automated process that assists in identifying or verifying an individual based on the physical characteristics of an individual's face." Balt. Code, Police § 18-1(b).

Core Compliance Requirement

Under the Baltimore FRT Ordinance, persons are prohibited from obtaining, retaining, accessing, or using any face surveillance system, or any information obtained from a face surveillance system, within the boundaries of Baltimore City. Balt. Code, Police § 18-2.

Enforcement and Penalties/Damages

The Baltimore FRT Ordinance is enforced through the imposition of criminal penalties. See Balt. Code, Police § 18-3. Specifically, any person who violates the ordinance is guilty of a misdemeanor and subject to a fine of up to $1,000, imprisonment of up to 12 months, or both. Balt. Code, Police § 18-3(a). Each day that a violation continues constitutes a separate violation of the ordinance. Balt. Code, Police § 18-3(b).

Federal Trade Commission

Overview

In the absence of any federal privacy or security law, the FTC has long maintained the role as the country's de facto privacy and security regulator at the federal level. Generally, the FTC pursues privacy and security enforcement actions against organizations for violations of consumers' privacy rights or misleading or deceptive statements relating to the security of consumers' sensitive data. More recently, the FTC has made aggressively policing the misuse of facial recognition a top priority-significantly raising the liability risks associated with this increasingly popular form of biometrics.

Increased Policing of Improper Facial Recognition Practices

In early 2021, the FTC settled its first *enforcement action* specifically targeting improper facial recognition practices with photo developer Everalbum, Inc. (Everalbum). The enforcement action was a watershed event in the area of facial biometrics-demonstrating the wide scope of liability exposure that exists for companies utilizing facial recognition that extends well beyond the patchwork of various biometric privacy statutes and ordinances. In announcing the settlement, the FTC also offered an unequivocal warning that policing facial recognition technology will remain one of the FTC's top priorities for the foreseeable future.

Shortly after the Everalbum settlement-during remarks made at the 2021 Future of Privacy Forum-the FTC's then-Acting Chair, Rebecca Kelly Slaughter, emphasized that the FTC would "redouble" its efforts to identify facial recognition violations, particularly due to the significant discrimination and bias-related concerns regarding this technology and the obvious privacy implications of tools that are able to determine the identities of otherwise unknown individuals.

Mitigating Legal Risks When Using Biometric Data

There are several key, actionable steps that can be taken to effectively leverage biometric data in a way that satisfies all applicable legal requirements and mitigates legal risks. Implementing the following measures to enhance current compliance programs will enable your client to satisfy current biometric privacy laws and quickly pivot and adapt to new laws and requirements.

Determine Applicability

As an initial step, companies need to evaluate whether they collect and/or possess actual biometric data that falls under the scope of-and thus requires compliance with-today's biometric privacy laws.

Data Inventory

It is critical to understand *how* and *why* biometric data is collected, used, and managed in order to comply with legal obligations and minimize risk. Therefore-assuming that biometric data is collected and/or possessed-organizations must first complete a data mapping and inventory exercise.

This task involves mapping and inventorying all biometric data that is collected, possessed, used, stored, disclosed, and/or sold, as well as all organizational biometric data processing activities. To create an organizational map and inventory, businesses will need to survey all aspects of their operations-from marketing to human resources to vendors-to determine all points where the entity collects or receives biometric data. From there, businesses need to map out how that data flows through the organization once it is initially collected, including any instances where the data is shared with any vendors or other third parties, as well as where the data is stored and maintained within the organization.

When completed properly, this data flow map and inventory will significantly aid compliance efforts, particularly:

- Proactively managing and safeguarding biometric data
- Preparing and implementing necessary privacy policies and notice disclosures
- Understanding when and how to obtain and document consent -and-
- Adhering to applicable data retention and destruction schedules and requirements

Privacy-by-Design

Companies should design and implement biometrics programs and services with consumer privacy as a top priority. This principle is commonly known as "privacy-by-design," which includes the embedding of privacy and security measures throughout the biometric technology/data life cycle.

In particular, companies should consider the following to further the principle of privacy-by-design:

- Default settings should be fashioned in a manner that users are not required to take any action to protect their privacy.
- Control and transparency should be integrated into processes to enable consumers to understand the retention, uses, and disclosures of their biometric data.
- Biometric technologies should offer consumers easy-to-use tools to exercise control over their biometric data.
- The collection and use of biometric data should be limited to what is necessary.
- Biometric data should be collected only for specific, explicit, and legitimate purposes.
- Biometric data should not be used or otherwise processed in a manner that is incompatible with the purposes disclosed to consumers at the initial time of collection. -and-
- All biometric privacy-related ethical issues-such as the potential for discrimination and bias-should be addressed prior to the deployment of biometric technologies.

Privacy Policy

Companies must ensure they are being transparent with customers and other consumers regarding their biometric data practices by implementing a detailed biometrics-specific privacy policy that:

- Gives clear notice that biometric data is being collected, used, stored, and/or shared

- Lists the type(s) of biometric data that are being collected, used, stored, and/or shared
- Explains how biometric data will be used, disclosed, and/or sold
- Describes security measures used to safeguard biometric data from unauthorized access, disclosure, or acquisition
- Includes the company's biometric data retention and destruction guidelines and schedule (discussed in more detail below)
- Strictly prohibits the disclosure of any individual's biometric data without their consent -and-
- Bans the company and its employees from selling or otherwise profiting from any biometric data

Organizational privacy policies must be made publicly available before any biometric data is collected or used. At a minimum, biometrics-specific privacy policies should be included in the entity's broader online privacy policy. Companies should also update their policies whenever material modifications are made to their biometric data processing or management practices.

Data Retention/Destruction Guidelines/Schedule

As indicated above, privacy policies must include information on the organization's data retention and destruction guidelines and schedule.

The specific retention and destruction schedules and limitations vary between major biometric privacy statutes. As a best practice, biometric data should be destroyed when the initial purpose for collecting the biometric data has been satisfied or, in the employment context, when the employment relationship ends. Destroying biometric data at the earliest feasible time can significantly limit liability exposure-especially in the data breach context.

Notice

Companies must provide conspicuous notice regarding the collection and use of biometric data before any such data is collected, captured, or otherwise used. Notices should provide at a minimum:

- That biometric data is being collected, used, shared/disclosed, and/or stored
- The specific purpose(s) for collecting and using biometric data
- The length of time over which biometric data will be retained or stored before it is permanently destroyed
- A brief summary of the protective measures used to safeguard biometric data
- That biometric data may be shared with vendors, service providers, or other third parties (if applicable) -and-
- How individuals can obtain additional information regarding the organization's biometric data practices

Where appropriate, or required by law, contextual and just-in-time notices may be necessary.

In addition to developing the notice itself, businesses must also implement mechanisms to ensure that notices are supplied to all individuals prior to the time their biometric data is collected or otherwise obtained.

Written Consent

Companies must obtain written consent from all individuals before collecting their biometric data. Here, it is important to remember to obtain consent in two distinct contexts:

- At or before the initial collection of biometric data -and-
- Prior to any subsequent disclosure of biometric data to any third party

To ensure that this consent requirement is satisfied, companies should develop and use a standardized written consent form authorizing the company, as well as its vendors and service providers, to collect, possess, use, store, and share biometric data for the purposes specified in the company's privacy policy and notice.

In signing the written consent, individuals should acknowledge that they have read the company's general biometric data policy as well as its more specific, individualized notice regarding the collection and use of biometric data. The language of the written consent form should also make clear that individuals agree to those policies and guidelines, as well as to the collection and use of their biometrics, including the company's ability to share their biometrics with any service providers or third-party vendors.

Prohibition on Selling or Profiting from Biometric Data

Companies must adhere to the prohibition on selling or otherwise profiting from biometric data that is a common element among the majority of U.S. biometric privacy laws. To accomplish this, companies must:

- Implement and adhere to a formal, written policy strictly barring any sale or other type of transaction that involves profiting from biometric data
- Maintain mechanisms to ensure no biometric data is sold or otherwise used for profit by the company or its employees, agents, or vendors -and-
- Educate all employees, agents, and vendors on the company's policy which strictly precludes any sale or other for-profit use of biometric data in the company's possession or control

Data Security

Companies must implement and maintain data security measures to protect all biometric data that is captured, used, possessed, and stored from improper disclosure, access, or acquisition. In particular, companies should consider implementing the following practices where feasible:

- Designate one or more employees to manage and oversee the company's biometric security program.
- Implement a specified retention period and permanently dispose of stored biometric data once it is no longer necessary for the purpose for which the data was collected.
- Ensure that all biometric data is encrypted, both while at rest and in transit.
- Store all biometric data separately from other types of personal information such as names, birthdates, and account numbers.
- Maintain stringent password protection policies for all individuals who have internal access to the systems that collect and use biometric data or the location(s) where such data is stored. This should encompass elements such as password expiration, complexity, and length.
- Have employees complete mandatory biometrics-focused security awareness training on the company's security program and policies, including best practices for employees:
    - To ensure that biometric data is stored, handled, and transmitted safely
    - To identify and avoid attempted cyberattacks targeting biometric data
- Perform periodic risk assessments to identify the primary risks to stored biometric data and modify the entity's information security program to minimize these risks.
- Perform penetration testing on the company's networks and systems to identify security vulnerabilities that could be exploited by hackers and modify the entity's information security program to minimize the risk of malicious actors exploiting these vulnerabilities.
- Implement network security monitoring tools to detect unauthorized access to biometric data, attempted cyberattacks, and other malicious behavior.

Vendor and Service Provider Risk Management

In addition to ensuring its own compliance, companies must take proactive steps to ensure its third-party biometrics vendors, service providers, and related entities maintain necessary security measures and protocols to safeguard the entity's sensitive data in their hands. Businesses should adhere to the following steps to avoid falling victim to a security incident while the company's sensitive biometric data is in the possession or control of the third party.

Due Diligence

Before entering into a relationship with any vendor that will have access to biometric data, companies should perform due diligence and vetting to ensure the vendor's security measures are sufficiently robust. The following are key due diligence areas that must be addressed when vetting any biometrics vendor:

- Implementation and maintenance of comprehensive, up-to-date security policies and incident response plans
- Performance of regular penetration testing and security audits -and-
- Completion of background checks on all vendor employees and other individuals who will be given access to the company's biometric data

Contractual Provisions

Companies should also ensure that all biometrics vendor and service provider contracts consider the principal issues raised by biometric privacy laws, including the risk of a security incident involving the entity's biometric data. The following are key contractual provisions that should be included in all such agreements:

- Prohibition on the disclosure or sale of biometric data
- Compliance with laws
- Minimum data security standards
- Security incident standards, cooperation, and reimbursement of remediation expenses
- Audit rights
- Limitation of liability -and-
- Indemnification

Monitoring and Audits

Lastly, companies must also ensure that their vendors and service providers maintain sufficient security measures and data handling practices over time through ongoing monitoring. All vendors and service providers should be reviewed periodically, such as through data security assessment questionnaires. Those holding more sensitive data, or higher-risk vendors / service providers, should be subject to a more extensive review. For these high-risk vendors and service providers, businesses should consider using third-party audits (which must be conducted by experienced biometric privacy counsel to ensure that the audit is covered by the attorney-client privilege) to ensure compliance with today's biometric privacy laws and industry best practices.

Arbitration Agreements and Class Action Waivers

Although not required by biometric privacy laws, companies should also ensure that they develop and utilize robust arbitration agreements and class action waivers to limit potential class action liability exposure in connection with the collection and use of biometric data.

The ability to resolve disputes through binding individual arbitration is an especially important tool for companies that face an ever-growing risk of high stakes biometric privacy class action litigation. Arbitration offers many benefits, including cost savings and prompt resolution of disputes.

Arbitration provisions can be used as a risk mitigation tool in a wide range of agreements, including employment agreements and online Terms of Use. When executed properly, arbitration provisions allow companies to compel individuals to resolve biometric privacy disputes individually and not in court.

Current as of: ***04/25/2022***

End of Document