JacksonLewis

Biometric Information Privacy: BIPA and Beyond

Privacy, Data and Cybersecurity

Fingerprints, facial geometry, voiceprints, and vein patterns in a person's palm are just a few examples of the kinds of biometrics maintained about individuals. Existing and emerging technologies increasingly leverage this data for a range of purposes, including without limitation validating one's identity, enhancing physical security, and enhancing or improving the customer experience.

About a $20 billion market in 2020, research suggests that the biometrics market is expected to grow to approximately $44 billion in 2026. This is not hard to imagine considering how ubiquitous biometric applications have become in everyday life - unlocking smartphones, accessing theme parks, operating cash registers, clocking in and out for work, and traveling by plane.

> *The simplest, most secure way to sign into your accounts without a password. Passkeys are an easier and more secure alternative to passwords. They let you sign-in with just your fingerprint, face scan, or screen lock.*
> – Google Safety Center

A common application of biometric-related technology is to permit individuals to log into their devices with the scan of a finger or a face. By some estimates, more than half of mobile device users unlock their devices with such a scan. At the same time, regulatory agencies have issued guidance and commentary surrounding the privacy and security of biometric data, including from the primary U.S. consumer protection agency, the Federal Trade Commission (FTC). In 2023, the FTC issued a policy statement addressing potential harm to consumers and violations of the FTC Act.

Until now, state law has been the primary driver of regulation of biometric information in the U.S., most notably the Illinois Biometric Information Privacy Act (BIPA), enacted in 2008. However, other states and cities have expanded protections for biometric information. See Jackson Lewis' Biometric Law Map for more information.

Despite how effective, convenient, and efficient these technologies may be, companies need to think through carefully their adoption and implementation.

These FAQs summarize the regulation of biometric information in the U.S.

In General

1. What is biometrics?

In general, biometrics is the measurement and statistical analysis of an individual's physical and behavioral characteristics. Examples of physiological characteristics include DNA, fingerprints, face, hand, retina or ear features, and odor. Examples of behavioral characteristics include gestures, voice, typing rhythm, and gait.

When it comes to compliance with the law, what constitutes a biometric identifier or biometric information must be evaluated carefully. Contrast the BIPA definition of biometrics with that of the California Consumer Privacy Act (CCPA):

BIPA

"Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.

"Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual.

Many technologies that have been the subject of litigation do not collect, use, or store a face scan or a fingerprint, but instead convert that information to a hash or other code that cannot be reverse-engineered to recreate the identifier – *e.g.*, the fingerprint. While the text of the BIPA may arguably suggest a broad interpretation, whether the statute applies to both the fingerprint and information converted from that identifier remains an unsettled issue that is the subject of ongoing litigation and which will ultimately be addressed by the courts.

CCPA

"Biometric information" means an individual's physiological, biological, or behavioral characteristics, including information pertaining to an individual's deoxyribonucleic acid (DNA), that is used or is intended to be used singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

2. How are biometrics used by organizations?

The use of biometric-related technologies by organizations has become widespread and new applications continue to emerge. Common uses include:

Time Management – Organizations across all industries have deployed time clocks which include login options that allow individuals to clock in and out by scanning their finger, face, eye, or hand, rather than an I.D. card or pin code – in order to save costs, eliminate time theft, and ensure more accurate compliance with time and attendance policies.

Security Access – One of the original and most common applications of biometric-related technology is to facilitate secure access. Typically through finger scanners, hand scanners, and facial scans, organizations use this technology to facilitate secure access to laptops, keyboards/mice, USB and portable storage devices, as well as for general physical security (access to buildings and spaces within). Iris and retina scanners are more expensive and generally justify use only in locations that require a high-security clearance.

Identity Verification – Many organizations have replaced traditional means of identity verification (*e.g.*, verbally confirming certain data elements such as date of birth and address) with more secure options, like biometric-related technologies. For example, voice technology has been leveraged by many financial institutions to protect customer accounts, such as those maintained under retirement plans, including 401(k) plans.

Health Plans – Biometrics assist health plans in establishing effective wellness programs. Biometric screening of an enrolled population allows data to be aggregated, providing a complete risk profile for each individual. Some plans also measure biometric data of individuals to assess their health risks and provide incentives for changing behaviors that could lower those risks.

3. Are there unique concerns with facial recognition technology and emerging deepfake applications?

A significant piece of the biometric-related technology market, facial recognition, has become increasingly popular in the employment and consumer space (*e.g.* employee access, passport check-in systems, payments on smartphones), as well as with law enforcement. For approximately twenty years, law enforcement has used facial recognition technology to aid with criminal investigations with mixed results, including claims of racial discrimination and disparate impact.

In addition to law enforcement, the COVID-19 pandemic helped to drive broader use of this technology. The need to screen persons entering a facility for symptoms of the virus, including temperature, led to increased use of thermal cameras, kiosks, and similar devices, many of which were embedded with facial scan capabilities. When federal and state unemployment benefit programs experienced massive fraud as they tried to distribute hundreds of billions in COVID-19 relief, many turned to facial recognition and similar technologies to help. By late summer 2021, more than half of the states in the U.S. have contracted with ID.me to provide identity verification services.

Many have objected to the use of this technology in its current form, however, citing concerns such as a lurch toward a more Orwellian society and due process, noting some shortcomings in accuracy and consistency. Others have observed the ability to compromise the technology as a potential new path to committing fraud against individuals.

Enter generative AI and deepfake technology. A product primarily of the porn industry, deepfakes are generated through feeding original content, including images, into deep learning AI to create fake content, whether in the form of manufactured images, videos, and/or sound. With security being a significant factor driving the use of biometrics, some have raised concerns that deepfakes could undermine biometric security.

The Illinois Biometric Information Privacy Act

4. What is the Illinois Biometric Information Privacy Act (BIPA)?

The Illinois Biometric Information Privacy Act, 740 ILCS 14 *et seq*. (BIPA), enacted in 2008, was one of the first state laws to address the collection and use of certain defined biometric identifiers and biometric information. The BIPA's comprehensive set of rules for companies that either possess or collect, capture, purchase, receive through trade, or otherwise obtain defined biometric identifiers or biometric information has five key features:

- Requires informed consent
- Permits a limited right to disclosure
- Mandates data protection and retention obligations
- Prohibits profiting from biometric data
- Creates a private right of action for "aggrieved" individuals and provides that a prevailing party may recover for each violation liquidated damages of $1,000 or actual damages (whichever is greater) against entities that negligently violate the Act, or liquidated damages of $5,000 or actual damages (whichever is greater) against entities that recklessly or intentionally violate the Act.

5. Does the BIPA apply to my organization?

In general, the BIPA applies to private entities that either "possess" biometric identifiers or biometric information (with respect to claims under Sections 15(a), (c), (d) and (e)), and private entities that collect, capture, purchase, receive through trade, or otherwise obtain biometric identifiers or biometric information (with respect to claims under Section 15(b)). See definitions in FAQ1 above.

Certain entities are excluded, including financial institutions that are subject to Title V of the federal Gramm-Leach-Bliley Act, and contractors, subcontractors, or agents of a State agency or local unit of government when working for that State agency or local unit of government.

6. What about healthcare entities?

Biometric identifiers under the BIPA do not include information captured from a patient in a healthcare setting or information collected, used, or stored for healthcare treatment, payment, or operations under HIPAA. By way of example, some hospitals have implemented a procedure whereby healthcare workers can access certain medications by allowing individuals to scan a finger or hand to access those medications. In *Mosby v. Ingalls Memorial Hospital*, a group of nurses argued that the BIPA only excludes patient information and that the hospitals violated the BIPA when they collected their alleged biometric data in connection with their use of such medication dispensing stations without consent.

The Illinois Supreme Court disagreed. The court held that the exemption at issue applies to any information "used for a particular purpose—health care treatment, payment, or operations—regardless of the information's source," as those functions (treatment, payment, or operations) are defined by HIPAA. The scope of the healthcare exemption under Section 10 of the BIPA is subject to ongoing litigation.

7. Is a scan of a finger, hand, face, or eye considered biometric information?

As noted above, the BIPA defines biometric information as any information, regardless of how it is captured, converted, stored, or shared that is based on an individual's biometric identifier used to identify an individual. Subject to a number of exceptions, a biometric identifier generally means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. While no appellate court has ruled on this point, plaintiffs regularly argue that a scan of a finger, hand, face, or eye fall within the scope of the statute. Organizations deploying this type of technology will need to examine the technology to determine whether biometric identifiers or biometric information as defined under the BIPA are being collected, stored, or used.

8. What is our organization's potential exposure for violating the BIPA?

Since the late 2010s, thousands of putative class actions have been filed under the Illinois statute.

The BIPA permits individuals "aggrieved" by violations of the Act to sue. If successful, they may recover for each violation liquidated damages of $1,000 or actual damages, whichever is greater, along with attorneys' fees and expert witness fees. The liquidated damages amount may increase to $5,000 if the private entity violates the Act intentionally or recklessly. In 2019, the Illinois Supreme Court ruled in *Rosenbach v. Six Flags Entertainment Corp*. that in order to qualify as an "aggrieved" person under the Act, an individual "need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act." Following the Illinois Supreme Court's decision in Rosenbach, the number of cases filed under the BIPA increased dramatically.

Surprised by the IL Supreme Court's interpretation of "aggrieved," many organizations wondered when a claim under Sections 15(b) and (d) of the BIPA accrues – *either once at the time* of first collection or disclosure, or with each purported collection or disclosure. That question was answered by the Illinois Supreme Court in 2023 in the *Cothron v. White Castle Systems* decision. In *Cothron*, the Illinois Supreme Court held that a new claim for a violation of Sections 15(b) and (d) of the BIPA can accrue *each time* the covered organization collects or discloses biometric identifiers or biometric information without consent.

The court in *Cothron* also made clear that the damages provision in the BIPA is discretionary, not mandatory. The majority noted, "[T]here is no language in the Act suggesting legislative intent to authorize a damages award that would result in the financial destruction of a business." The Court also stated, "[A] trial court presiding over a class action … would certainly possess the discretion to fashion a damage aware that (1) fairly compensated claiming class members and (2) included an amount designed to deter future violations, without destroying defendant's business." As of this writing, a bill that would reform how violations accrue under the BIPA, SB2979, advanced to the Governor's desk.

Of course, questions concerning standing, what constitutes a violation of the statute that will entitle an individual to seek and recover damages, and how finders of fact may exercise their discretion in awarding damages under the statute (if any) all remain open questions that are actively being litigated.

9. What is the statute of limitations for claims under the BIPA?

The Illinois Supreme Court addressed this issue in early 2023 in the *Tims v. Carriers, Inc*. decision, rejecting the argument that a one-year statute of limitations applies to claims under the BIPA and instead applying the default five-year limitations period applies. Notably, laches arguments – asserting relief should be denied to a claimant who unreasonably delayed in bringing a potential claim – still remain.

10. What best practices should our organization establish if it collects, stores, or uses biometric information?

First, confirm whether your organization is capturing biometric identifiers or biometric information as defined under applicable law. Remember that issues regarding the scope of the BIPA and whether data falls within the BIPA's definition of "biometric identifier" or "biometric information" are still the subject of ongoing litigation.

Notably, the Illinois Supreme Court stated in its *Rosenbach* decision:

> [c]ompliance should not be difficult; whatever expenses a business might incur to meet the law's requirements are likely to be insignificant compared to the substantial and irreversible harm that could result if biometric identifiers and information are not properly safeguarded; and the public welfare, security, and safety will be advanced.

Accordingly, organizations may want to consider the following when evaluating compliance with biometric-related laws, rules, or regulations:

- **Only collect the data needed.** This is a general collection principle for any type of personal information, not just biometrics. Biometrics of customers, clients, or employees should be collected and maintained for a lawful purpose directly related to the organization's functions and activities for which it was collected in the first place. The collection of biometrics should be necessary and not excessive for achieving this purpose. As with the collection of any potentially sensitive data, if this lawful purpose can be achieved by collecting other data or less potentially sensitive data, then consider whether only that data should be collected.

- **Retention of biometrics should be for no longer than is needed.** Similar to the consideration of "only collecting the information you need," a good rule of thumb is to avoid keeping personal information for longer than is needed. Under the BIPA, a private entity in possession of biometric identifiers and biometric information must establish a retention schedule and guidelines for permanently destroying the same when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three years of the individual's last interaction with the entity collecting it, whichever occurs first.

- **Establish a plan for accessing, storing, and safeguarding biometrics.** Before collecting biometrics, companies generally must provide notice and/or obtain written consent from the individual. The BIPA requires a "written release," which means informed written consent or, in the context of employment, a release executed by an employee as a condition of employment. As with other personal data, if it is accessible to or stored by a third-party service provider, the organization should obtain written assurances from that service provider concerning such things as minimum safeguards, record retention, and obligations in the event of a breach or unauthorized access or acquisition of that data.

- **Implement appropriate safeguards.** In general organizations should develop and implement reasonable administrative, technical, and physical safeguards to protect personal information. Specifically, under BIPA, entities in possession of biometric identifiers or biometric information must store, transmit, and protect from disclosure all biometric identifiers and biometric information: (a) using the reasonable standard of care within the entity's industry, and (2) in a manner that is the same as or more protective than the manner in which the entity stores, transmits, and protects other confidential and sensitive information.

- **Review compliance periodically.** If a biometrics compliance plan is already in place, whether under the BIPA or otherwise, the organization should review its time management, point-of-purchase, device access, physical security, or other systems that may potentially obtain, use, or disclose biometric data against the requirements under the law periodically. Over time, technology and procedures could change, even if unintentionally. In the event technical or procedural gaps in compliance are found, steps to remedy those gaps should be taken.

- **Prepare to handle a breach involving biometric data.** Illinois' data breach notification law requires notification of a breach of "personal information," including biometric information. Accordingly, companies should include biometric data as part of their written incident response plans. Notably, BIPA's definition of biometric information is not necessarily the same as under Illinois' breach notification law. The breach notification law protects "Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data." As noted above, whether biometric information as defined by the BIPA would implicate the breach notification law in Illinois, remains to be seen.

11. Do I need consent from an employee in order to collect, use, or disclose biometric identifiers or biometric information?

In Illinois, under the BIPA, "no private entity may collect, capture, purchase, receive through trade, or otherwise obtain" a person's or a customer's biometric identifier or biometric information as those terms are defined under the statute unless it first:

- informs the individual or the individual's legally authorized representative in writing (i) that a biometric identifier or biometric information is being collected or stored, and (ii) of the specific purpose and length of term for which such biometric identifier or biometric information is being collected, stored, and used; and
- Receives a written release executed by such individual or representative.

The BIPA defines a "written release" as "informed written consent or, in the context of employment, a release executed by an employee as a condition of employment." We can provide a sample form for this purpose, if needed, which would need to be customized based on applicable law, your practices, and the type of technology at issue.

Regulation of Biometric Information in Other States

12. Have other jurisdictions enacted laws similar to the BIPA?

Colorado, Texas and Washington have enacted comprehensive biometric laws similar to the BIPA but without a private right of action. Other states, such as New York, have considered BIPA-like privacy bills that mirrored the BIPA's enforcement scheme, but without success. New York City passed a couple of industry-specific measures to safeguard biometric information, which include private rights of action.

Colorado. When Colorado enacted the Colorado Privacy Act (CPA), it included "biometric data that may be processed for the purpose of uniquely identifying an individual." However, the CPA as originally drafted did not cover the personal data of individuals acting in a commercial or employment context. Last week, Colorado amended the CPA to broaden the protections for biometric data when Gov. Jared Polis signed HB-1130 into law.

Importantly, HB-1130 alters the scope of the CPA's application. Recall that under the CPA, a controller is subject to the CPA if it:

(i) determines the purposes and means of processing personal data, (ii) conducts business in Colorado or produces or delivers commercial products or services intentionally targeted to residents of the state, and (iii) either: (a) controls or processes the personal data of more than 100,000 Colorado residents per year or (b) derives revenue from selling the personal data of more than 25,000 Colorado residents.

HB-1130 adds that a controller can be subject to the CPA without meeting the requirements above, provided that it would be subject to the CPA solely to the extent that it controls or processes any amount of biometric identifiers or biometric data.

The amendment added language expressly applicable to employers, including defining employees to include not only individuals employed on a full or part time basis, but also individuals who are "on-call" or hired as a "contractor, subcontractor, intern, or fellow." The amendment also adds definitions for biometric data and biometric identifier,

> *"Biometric data" means one or more biometric identifiers that are used or intended to be used, singly or in combination with each other or with other personal data, for identification purposes. "Biometric data" does not include the following unless the biometric data is used for identification purposes: (i) a digital or physical photograph; (ii) an audio or voice recording; or (iii) any data generated from a digital or physical photograph or an audio or video recording.*
>
> *"Biometric identifier" means data generated by the technological processing, measurement, or analysis of a consumer's biological, physical, or behavioral characteristics, which data can be processed for the purpose of uniquely identifying an individual. "Biometric identifier" includes: (a) a fingerprint; (b) a voiceprint; (c) a scan or record of an eye retina or iris; (d) a facial map, facial geometry, or facial template; or (e) other unique biological, physical, or behavioral patterns or characteristics.*

While there are some similarities in these definitions to the corresponding definitions in the popular Illinois Biometric Information Privacy Act (BIPA), there are some significant differences. One is that a biometric identifier under the BIPA is defined as a "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." The Illinois law does not make reference to "other unique biological, physical, or behavioral patterns or characteristics." There is also not a private right of action for violations of the CPA amendment, as there is in the BIPA.

HB-1130 establishes several requirements for controllers that control or process one or more biometric identifiers. These requirements include:

- Obtaining consent from the consumer (including the employee) before collecting the consumer's biometric data.
- A written policy that
    - Establishes a retention schedule for biometric identifiers and biometric information,
    - Includes a process for responding to the data security incident that would compromise the security of biometric identifiers or biometric information. This would include the process for notifying consumers under the state's existing data breach notification law.
    - Establishes guidelines addressing the deletion biometric identifiers within certain time frames.
- Subject to certain exceptions, controllers must make the written policy available to the public. One exception is for a policy applying only to current employees of the controller.
- Providing a reasonably accessible, clear, and meaning privacy notice satisfying specific content requirements including the purposes for processing.
- Satisfying certain rights the consumer may have with respect to their biometric data, including the right to access.

HB-1130 also prohibits controllers from certain activities concerning biometric identifiers such as:

- Selling, leasing or trading such information,
- Disclosing biometric identifiers, subject to limited exceptions including consent and complying with federal or state law.
- Refusing to provide a good or service to a consumer, based on the consumer's refusal to consent to the controller's collection, use, disclosure, etc. of a biometric identifier unless same is necessary to provide the good or service.

Controllers and processors also must use a reasonable standard of care when storing, transmitting, and protecting biometric identifiers from disclosure.

HB-1130 includes certain specific provisions for employers. While the law provides that employers may require current or prospective employees to allow the employer to collect and process their biometric identifiers, they may do so only to

- Permit access to secure physical locations and secure electronic hardware and software applications (but not obtain consent to retain such data for current employee location tracking or tracking time using a hardware or software application),
- Record the commencement and conclusion of the employee's full workday, including meal breaks and rest breaks in excess of 30 minutes,
- Improve or monitor workplace safety or security or ensure the safety or security of employees,
- Improve or monitor the safety or security of the public in the event of an emergency or crisis situation.

Collecting or processing biometric identifiers for other purposes will require consent which satisfied the applicable CPA requirements. However, employers will be able to collect and process biometric identifiers where the anticipated uses are "aligned with the reasonable expectations" of an employee based on the employee's job description or role, or a prospective employee based on reasonable background check, application or identification requirements.

Texas. The Texas law protects "biometric identifiers," defined as either a "retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry." This definition is a bit narrower than the scope of data protected under the BIPA, although the Lone Star state's law includes similar requirements as the BIPA – notice and consent, maximum retention period (1 year, instead of 3 years in the Illinois statute), prohibitions on sale or disclosure without consent, and reasonable safeguards. Unlike the BIPA, there is no private right of action. The state's attorney general may bring an action for civil penalties of not more than $25,000 for each violation.

Washington. Effective July 23, 2017, Washington's biometric data protection statute defines "biometric identifiers" to mean:

> *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. "Biometric identifier" does not include a physical or digital photograph, video or audio recording, or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996.*

It prohibits persons from "enrolling" biometric identifiers in a database for a "commercial purpose" without first providing notice, obtaining consent, or providing a mechanism to prevent the subsequent use of the biometric identifiers for a commercial purpose.

"Enroll" means "to capture a biometric identifier of an individual, convert it into a reference template that cannot be reconstructed into the original output image, and store it in a database that matches the biometric identifier to a specific individual." And "commercial purpose" means, "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 or services are unrelated to the initial transaction in which a person first gains possession of an individual's biometric identifier." Considering the scope of the commercial purpose definition, the Washington law does not appear to apply in an employment context, such as with time management devices, which have led to significant litigation in Illinois. It remains to be seen whether a court will agree.

The exact type of notice and consent will depend on the context, and notice must be given through a procedure reasonably designed to be readably available to affected individuals. Also, in general, a person who has obtained a biometric identifier from an individual and enrolled that identifier, may not sell, lease, or otherwise disclose the identifier absent consent. Persons that possess biometric identifiers of individuals that have been enrolled for a commercial purpose must (i) have reasonable safeguards to protect against unauthorized access or acquisition to the identifiers, and (ii) not retain the identifiers for longer than is necessary to carry out certain functions, such as providing the product for which the identifier was acquired.

There is no private right of action under the Washington law. As in Texas, it is enforced by the state's attorney general.

New York City. The Big Apple took a more targeted approach to regulating biometric information in the City while retaining a private right of action similar to the BIPA.

First, it amended Title 22 of its Administrative Code to create BIPA-like requirements for the retail, restaurant, and entertainment businesses relating to collecting customers' "biometric identifier information" – that is, "a 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." Notably, this definition is not limited to the listed physiological or biological characteristics.

The law has two primary requirements – (i) provide clear and conspicuous signage of the collection, retention, conversion, storage, or sharing of biometric identifier information to customers, and (ii) do not sell, lease, trade, share in exchange for anything of value or otherwise profit from transactions involving biometric identifier information. Under the law, customers have a private right of action to remedy violations, subject to a 30-day notice and cure period, with damages ranging from $500 to $5,000 per violation, along with attorneys' fees.

Next, New York City passed the Tenant Privacy Act, which, among other things, requires owners of "smart access" buildings – *i.e.*, those that use key fobs, mobile apps, biometric identifiers, or other digital technologies to grant access to their buildings – to provide privacy policies to their tenants prior to collecting certain types of data from them, as well as to strictly limit (a) the categories and scope of data that the building owner collects from tenants, (b) how the covered entities use that data (including a prohibition on data sales), and (c) how long the information may be retained. The law creates a private right of action for tenants whose data is unlawfully sold. Those tenants are empowered to seek either compensatory damages or statutory damages ranging from $200 to $1,000 per tenant, along with attorneys' fees.

13. What about the emerging comprehensive state privacy laws, like the California Consumer Privacy Act? Do they cover biometric information?

Yes, these laws do cover biometric information to one degree or another. While a complete summary of those laws is beyond the scope of these FAQs, we summarize the treatment of biometric information by the California Consumer Privacy Act (CCPA).

Modeled to some degree after the EU's General Data Protection Regulation (GDPR), comprehensive privacy laws have emerged in several states in the United States, most notably the CCPA. The CCPA seeks to provide individuals who are residents of California (consumers) greater control over their personal information. That control is provided through, among other things, requirements on covered businesses to provide notice about data collection practices, to maintain a website privacy policy, and to extend an expanding array of rights, including the right to delete and limit the use of personal information.

The CCPA defines personal information broadly and sets out several non-exhaustive categories of personal information, one being "biometric information" which is defined to mean an individual's:

> *physiological, biological, or behavioral characteristics, including information pertaining to an individual's deoxyribonucleic acid (DNA), that is used or is intended to be used singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.*

It is worth noting that, in certain respects, biometric information covered by the CCPA is significantly broader than the kinds of information covered under the BIPA and some of the other laws discussed above. Additionally, the California Privacy Rights Act (CPRA) amended the CCPA to add a new category of personal information – "sensitive personal information" – which is defined to include certain biometric information. Sensitive personal information comes with specific protections including the right to limit uses and disclosures of that information under certain circumstances.

There is no private right of action under the CCPA for most violations of the law. However, if a CCPA-covered business experiences a data breach involving a subset of personal information, *which includes biometric information*, the CCPA authorizes a private cause of action against the business if a failure to implement reasonable security safeguards caused the breach. If successful, a plaintiff can seek to recover statutory damages in an amount not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is greater, as well as injunctive or declaratory relief and any other relief the court deems proper.

14. Are there other laws that regulate biometric information?

Whether biometric technologies are used in tracking employees' time management, authenticating a transaction, creating a profile for a wellness program, or using facial scans for marketing purposes, they may involve the collection, maintenance, and disclosure of personally identifiable information. There are many laws that seek to protect personal information, which in many cases may include biometric information. A full discussion and analysis of those laws is, again, beyond the scope of these FAQs, however, we have provided several additional examples of laws addressing the processing of biometric information.

- **Federal Nondiscrimination Law.** When using biometric information, notice, consent, safeguards, and retention rules may not be sufficient to avoid liability. Earlier in 2013, the U.S. Equal Employment Opportunity Commission (EEOC) claimed an employer's process for using a time clock that allowed employees to clock in or clock out by scanning their hands violated federal law by failing to accommodate certain religious beliefs that opposed the use of such devices. The case resulted in a jury verdict in excess of $500,000.

  Retinal scan technology is another technology that can be used to verify identity/security purposes. However, as explained in a recent Biometric.com article, "examining the eyes using retinal scanning can aid in diagnosing chronic health conditions such as congestive heart failure and atherosclerosis...[as well as] diseases such as AIDS, syphilis, malaria, chicken pox and Lyme disease [and] hereditary diseases, such as leukemia, lymphoma, and sickle cell anemia." Thus, the data captured by such scans can provide information about individual health conditions, raising a range of medical privacy, medical inquiry, and discrimination issues under federal and state laws.

- **Bans on collecting biometrics.** In New York, Labor Law Section 201-a prohibits the *mandatory* fingerprinting of employees by private employers, unless required by law. However, according to an opinion letter issued by the State's Department of Labor on April 22, 2010, a device that measures the geometry of the hand is permissible as long as it does not scan the surface details of the hand and fingers in a manner similar or comparable to a fingerprint.

  Over the past few years, several states, cities, and localities have banned the use of facial recognition by law enforcement. These include Vermont, Virginia, San Francisco, Boston, New Orleans, and Minneapolis.

  In September 2020, the City of Portland in Oregon became the first city in the United States to ban the use of "facial recognition technologies" in the *private sector*. Proponents of the measure cited, among other things, a lack of standards for the technology and wide ranges in accuracy and error rates that differ by race and gender.

  The term facial recognition technologies is broadly defined under the Portland Ordinance to include automated or semi-automated processes using face recognition that assist in identifying, verifying, detecting, or characterizing the facial features of an individual or capturing information about an individual based on an individual's face. The Ordinance carves out limited exceptions including the use of facial recognition technologies to comply with the law, and verifying users of personal and employer-provided devices, and social media applications. The Ordinance provides persons injured by a material violation a cause of action for damages or $1,000 per day for each day of violation, whichever is greater.

  The City of Baltimore also banned the use of facial recognition technologies by city residents, businesses, and most of the city government (excluding the city police department) until December 2022. Council Bill 21-0001 prohibits persons from "obtaining, retaining, accessing, or using certain face surveillance technology or any information obtained from certain face surveillance technology." Any person who violates the Ordinance is guilty of a misdemeanor and, on conviction, is subject to a fine of not more than $1,000 or imprisonment for not more than 12 months or both fine and imprisonment.

In New York, pursuant to a determination by New York State Education Department Commissioner Betty A. Rosa, K-12 schools are prohibited from purchasing or utilizing facial recognition technology. However, schools can decide whether to use biometric identifying technology other than facial recognition technology at the local level so long as they consider the technology's privacy implications, impact on civil rights, effectiveness, and parental input.

- **Safeguarding biometric information.** Several states, including California, Illinois, and New York require reasonable safeguards to be in place when storing, transmitting, and/or disclosing biometric information. Regardless of whether a statute or regulation requires an organization to safeguard biometric information, we believe it is a best practice to do so. Biometric information should be covered under the organization's written information security program. In addition, organizations should consider the steps vendors are taking to safeguard the biometric information the vendors process on their behalf and have written assurances from the vendor concerning the safeguarding of that information.
- **Notification requirements in the event of a breach of biometric information.** All fifty states have a data breach notification law concerning breaches affecting "personal information." Several of those states include biometric information in their definition of personal information. Accordingly, for states such as Michigan, a data breach involving biometric information may require notification to affected individuals. MCLS § 445.72.
- **Proper disposal of biometric information.** A number of states (*e.g.*, Colorado and Massachusetts) require that certain entities meet minimum standards for properly disposing of records containing biometric information.

Contacts

Joseph J. Lazzarotti
Principal

Tampa
908-795-5205
Joseph.Lazzarotti@jacksonlewis.com

Jason C. Gavejian
Office Managing Principal

Berkeley Heights
908-795-5139
Jason.Gavejian@jacksonlewis.com

Jody Kahn Mason
Principal

Chicago
312-803-2535
Jody.Mason@jacksonlewis.com

Jason A. Selvey
Principal

Chicago
312-803-2513
Jason.Selvey@jacksonlewis.com

Learn more: Privacy, Data and Cybersecurity practice group