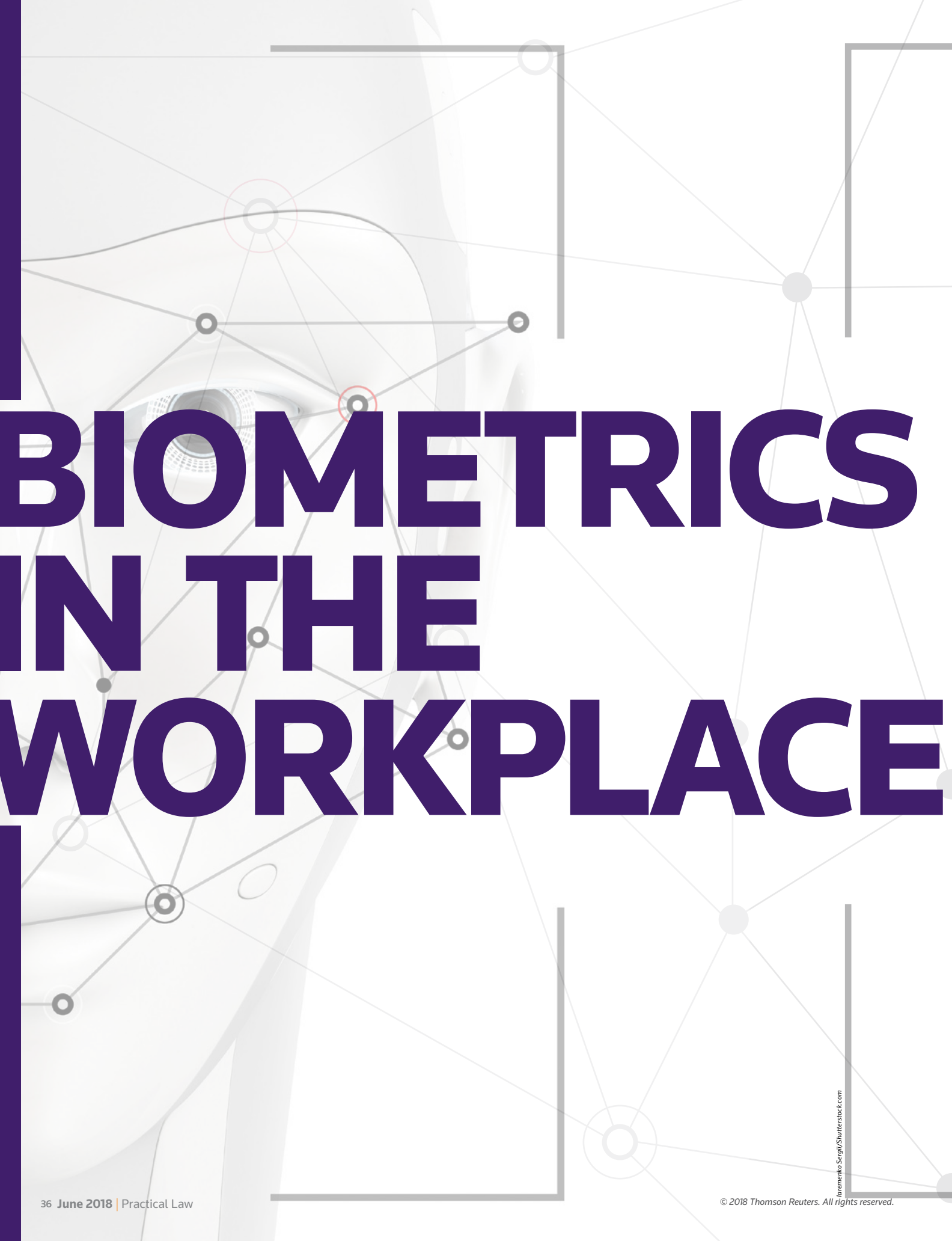
BIOMETRICS IN THE WORKPLACE



Iaremenko Sergii/Shutterstock.com

SUSAN GROSS SHOLINSKY
MEMBER
EPSTEIN BECKER & GREEN, P.C.

Susan is a Member of the firm in the Employment, Labor & Workforce Management practice. She advises employers on all facets of the employment relationship, develops and audits policies and procedures, counsels on the avoidance of employment-related disputes, prepares employment, consulting, separation, and non-compete agreements, conducts workplace training seminars, performs company-wide audits regarding wage and hour issues, and represents employers in discrimination, wrongful discharge, harassment, and employment contract cases.

BARBARA J. HARRIS
SENIOR LEGAL EDITOR
PRACTICAL LAW

Barbara is a Senior Legal Editor on the Practical Law Labor & Employment team, with significant experience counseling employers on all aspects of the employment relationship and litigating employment disputes in federal and state court. Previously she was counsel in the labor and employment group at DLA Piper LLP (US), counsel at Solomon, Zauderer, Ellenhorn, Frischer & Sharp, and a litigation associate at Alschuler, Grossman & Pines LLP.

Employers are increasingly using employees' biometric information for a variety of human resources and other business functions. However, recent class action lawsuits under state biometric privacy laws, along with proposed and pending biometric legislation, have highlighted the risks to employers that collect and use this information. Employers must understand the evolving legal landscape governing biometrics to mitigate potential liability.

Employers nationwide are increasingly using biometric information for authentication, security purposes, and recording employee worktime. A March 2018 survey by Spiceworks (available at *community.spiceworks.com*) suggests that 62% of all companies use biometrics in some capacity in the workplace, with that number likely rising to 90% by 2020.

Although several federal statutes address privacy and data security breach protections generally, no comprehensive federal law currently addresses an employer's obligations regarding the use or disclosure of its employees' biometric information. However, several states have passed laws specifically regulating biometric privacy. Recent class action lawsuits under the Illinois Biometric Information Privacy Act (BIPA) and the enactment of a biometric privacy law by Washington State in 2017, combined with legislation proposed or pending in other jurisdictions, has brought this issue to the forefront for employers that collect and use biometric information.

To assist employers and employment counsel in understanding and complying with the changing legal landscape governing biometrics in the workplace, this article:

- Provides an overview of biometrics, including common uses of biometric information in the workplace.

- Analyzes and compares existing and proposed legislation governing biometric privacy.
- Discusses recent trends and developments in biometrics litigation.

BIOMETRICS BASICS

Employers should understand:

- The definition of biometrics and other key terminology.
- The three basic steps of the biometric process.
- Common uses of biometrics in the workplace.

DEFINITIONS AND TERMINOLOGY

While there is no universally accepted definition, the term biometrics usually refers to either:

- Measurable human biological and behavioral characteristics that can be used for identification.
- The automated methods of recognizing or analyzing an individual based on human biological and behavioral characteristics.

Biometrics are a subset of, but distinct from, personal information, which is defined in many statutes and is much broader. Biometrics are different from other personally identifiable information collected from employees. Unlike other information, such as social security numbers, which can be changed if compromised, employees cannot change their biometrics. According to BIPA, biometrics are "biologically unique to the individual; therefore, once compromised, the individual has no recourse ... [and] is at heightened risk for identity theft" (740 ILCS 14/5(c)). For this reason, biometric data and information may warrant greater protections (and penalties for violating those protections) than misuse or theft of other personal information.

Biometric identifiers are data generated by automatic measurements of an individual's biological characteristics. Biometric information is information derived from biometric identifiers. Although statutory definitions vary, biometric identifiers may include raw images such as:

- Retina or iris scans.
- Fingerprints.
- Voiceprints.
- Scans or records of hand or face geometry.
- DNA.
- Palm prints.
- Palm veins.
- Other unique biological characteristics used to identify a specific individual.

The term biometric identifier generally does not include:

- Written signatures.
- Biological samples used for testing.
- Demographic data.
- Physical descriptions.
- Films or images of the human anatomy, such as X-rays or MRIs.

THE BIOMETRIC PROCESS

The three basic steps of the biometric process are:

- **Enrollment or registration.** This is the process of collecting a biometric sample (such as a fingerprint or voice recording) from an individual.
- **Template generation.** This is the process of generating a template (an encrypted biometric "key" or mathematical representation) from the sample that is specific to that individual. Many systems delete the raw images for security and privacy reasons, and templates are generally protected by encryption. Even if an encryption algorithm is broken, the template in its raw form is a mathematical representation that cannot be transformed into the original image.
- **Matching.** This is the process of comparing a live biometric sample against one or more templates in the biometric system database.

The two primary uses of biometric information are:

- **Identification of individuals (to answer the question "who are you?").** In this application, the biometric system compares a sample against a database and conducts a "one-to-many" matching search. This application is used most commonly in the government or law enforcement context.
- **Authentication of individuals (to answer the question "are you really who you say you are?").** In this application, the system compares user input to the individual's template and conducts a "one-to-one" matching search to determine if there is a match between the two. This application is commonly used for security purposes.

COMMON USES OF BIOMETRICS IN THE WORKPLACE

Employers have been using biometrics with increasing frequency for various human resources (HR) and business functions, primarily for authentication rather than identification. Common uses by employers include:

- **Timekeeping.** This includes using fingerprints or hand scans to punch in and out on biometric timeclocks, to avoid time theft and "buddy punching."
- **Electronic security and building access.** This includes using retina scans, facial recognition, or fingerprinting technology to control access to an employer's physical facilities, instead of using passwords or traditional ID cards.
- **Accessing employer-provided workplace equipment.** This includes accessing computer systems, copiers, and applications on laptops, tablets, and smartphones, using facial recognition or fingerprinting technology.
- **Safety and security.** This includes creating detailed employee profiles to track compliance and training.
- **Immigration compliance.** This includes using a biometric scanner to ensure that workers are legally authorized to work in the US.

In addition, some employers or their health plan providers conduct biometric screenings of their employees as part of a broader health or wellness program or initiative.

Search Wellness Programs for more on wellness and preventive care programs and considerations in designing these programs.

As technology evolves and the cost of collecting and processing biometric information decreases, employers may find new uses for biometric information in their HR functions.

EXISTING AND PROPOSED LEGISLATION

Employers considering using biometrics in the workplace should review:

- Federal statutes addressing employee privacy generally.
- State biometric privacy statutes.
- Additional laws affecting biometric information.
- Proposed legislation.

FEDERAL PRIVACY FRAMEWORK

Currently no single federal statute specifically addresses an employer's obligations regarding the collection, use, or retention of biometric information. Several other federal statutes, however, address employee privacy in various contexts. For example:

- The Health Insurance Portability and Accountability Act (HIPAA) addresses requirements for the protection of individually identifiable health information (IIHI) and protected health information (PHI) (though PHI does not include employment records held by an employer) (for more information, search HIPAA Privacy Rule).
- The Genetic Information Nondiscrimination Act (GINA) prohibits, among other things, employers from requesting, requiring, or buying an employee's genetic information or that of an employee's family member (for more information, search Discrimination Under GINA: Basics and GINA Compliance for Health and Welfare Plans).
- The Fair Credit Reporting Act (FCRA) imposes certain requirements and restrictions on employers conducting background checks (for more information, search Background Checks and References).

Employers with employees, customers, or business operations in the European Union (EU) also must comply with the General Data Protection Regulation ((EU) 2016/679) (GDPR), effective May 25, 2018.

Search Overview of EU General Data Protection Regulation for more on the GDPR.

STATE BIOMETRIC PRIVACY STATUTES

An employer's obligations regarding biometric information depend on where the employer is located and where it employs workers. To date, three states (Illinois, Texas, and Washington) have passed laws specifically governing the collection, use, disclosure, and destruction of biometric information. They are:

- The Illinois Biometric Information Privacy Act (BIPA) (740 ILCS 14/1 to 14/99).
- The Texas Capture or Use of Biometric Identifier Act (CUBI) (Tex. Bus. & Com. Code Ann. § 503.001).
- Washington State's law regarding biometric identifiers (RCW 19.375.010 to 19.375.900).

Other states have considered similar legislation, though these proposals have not gained much traction. Some amendments also have been proposed to existing legislation (see below *Proposed Legislation*).

While the existing and proposed statutory requirements and restrictions differ, common themes include:

- Requiring some form of notice that biometric information is being collected and how it is being used.
- Requiring clear consent from the individuals, sometimes in writing.
- Restricting to various degrees the selling, leasing, or other disclosure of biometric information.
- Providing standards for confidentiality, retention, and disposal when the biometric information is no longer needed for any purpose for which it was collected.

The following summarizes and compares the key provisions of the Illinois, Texas, and Washington laws, including:

- The scope of coverage.
- Important definitions.
- Notice and consent.
- Restrictions on sale, use, and disclosure.
- Storage, retention, and destruction.
- Remedies.

As technology evolves and the cost of collecting and processing biometric information decreases, employers may find new uses for biometric information in their HR functions.

Scope of Coverage

BIPA was the first state biometric statute enacted and has been in effect since 2008 (740 ILCS 14/1 to 14/99). BIPA applies to all private entities, but does not cover:

- State or local government agencies.
- Any court of Illinois, court clerk, or judge.

(740 ILCS 14/10.)

CUBI has been in effect in Texas since 2009 and is similar to BIPA, with a few variations (Tex. Bus. & Com. Code Ann. § 503.001). Although CUBI applies to all private entities, it only covers biometric identifiers used for a commercial purpose (Tex. Bus. & Com. Code Ann. § 503.001(b)). However, CUBI does not define the term commercial purpose. Absent further guidance, employers should assume that a commercial purpose may include, and that CUBI therefore covers, employers that gather biometric information to:

- Assist them in running their business efficiently.
- Accurately pay their employees.

CUBI specifically recognizes that biometric identifiers may be collected "for security purposes by an employer," but does not specify whether a security purpose constitutes a commercial purpose (Tex. Bus. & Com. Code Ann. § 503.001(c)(3)(c-2)).

Washington's biometric information law became effective in July 2017 (RCW 19.375.010 to 19.375.900). Similar to CUBI, it only applies to biometrics used for a commercial purpose, and covers all persons and entities except:

- A government agency (RCW 19.375.010(7)).
- A financial institution covered by Title V of the Gramm-Leach-Bliley Act and its rules (RCW 19.375.040(1)).
- Activities subject to HIPAA and its rules (RCW 19.375.040(2)).
- Law enforcement activities under the authority of state law, including lawful searches and seizures (RCW 19.375.040(3)).

Although broader than BIPA and CUBI in some respects, Washington's law only applies to biometric identifiers that are both:

- Enrolled, meaning those that have undergone the process of:
  - capturing a biometric identifier;
  - converting it into a reference template that cannot be reconstructed into the original output image; and
  - storing it in a database that matches the biometric identifier to a specific individual.

  (RCW 19.375.010(5).)
- Used for a commercial purpose, which by definition does not include a security or law enforcement purpose (RCW 19.375.020(1); 19.375.010(4), (8)).

Definitions

The definition of biometric identifier in each statute shares a common core, but varies in its exceptions and overall scope.

BIPA defines biometric identifier as a:

- Retina or iris scan.
- Fingerprint.
- Voiceprint.
- Scan of hand or face geometry.

(740 ILCS 14/10.)

BIPA's definition of biometric identifier specifically excludes:

- Writing samples and written signatures.
- Photographs.
- Human biological samples used for valid scientific testing or screening.
- Demographic data.
- Tattoo descriptions.
- Physical descriptions, such as:
  - height;
  - weight;
  - hair color; or
  - eye color.
- Donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act (755 ILCS 50/1-10).
- Blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency.
- Biological materials regulated under the Illinois Genetic Information Privacy Act (410 ILCS 513/1 to 513/50).
- Information:
  - captured from a patient in a health care setting; or
  - collected, used, or stored for health care treatment, payment, or operations under HIPAA.
- X-rays, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used:
  - for medical diagnosis, prognosis, or treatment; or
  - to further validate scientific testing or screening.

(740 ILCS 14/10.)

BIPA further defines biometric information as any information based on an individual's biometric identifier used to identify an individual (740 ILCS 14/10). Biometric information excludes information derived from the same items or procedures excluded under the definition of biometric identifier.

As interpreted by the courts, a biometric identifier under BIPA is a set of measurements used to identify a person, while biometric information is a conversion of those measurements into a different, usable form (*Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1096 (N.D. Ill. 2017)). It remains unclear, however, whether photographs (or information derived from photographs) are considered to be biometric identifiers. To date, courts have rejected arguments attempting to exclude from BIPA's definition all biometric information derived from photographs.

For example, the US District Court for the Northern District of California, applying Illinois law, held that a digital image of a person's face geometry could be considered a biometric identifier under BIPA (*In re Facebook Biometric Info. Privacy Litig.*, 185 F. Supp. 3d 1155, 1171 (N.D. Cal. 2016) (noting that the definition's exclusion of photographs is better understood

to mean paper prints of photographs, not digitized images stored as a computer file and uploaded to the internet); see also *Monroy v. Shutterfly, Inc.*, 2017 WL 4099846, at *3-4 (N.D. Ill. Sept. 15, 2017) (excluding biometric identifiers derived from photographs would mean that a "scan of face geometry" is limited to an in-person scan, which interpretation has no support in the statutory language or legislative history); *Gullen v. Facebook, Inc.*, 2018 WL 1609337, at *2-3 (N.D. Cal. Apr. 3, 2018) (assuming, without deciding, that BIPA covers biometric identifiers derived from photographs, but dismissing the case because the plaintiff's photograph did not actually undergo facial recognition)).

CUBI affirmatively defines biometric identifier the same as BIPA does, namely, as a:

- Retina or iris scan.
- Fingerprint.
- Voiceprint.
- Record of hand or face geometry.

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

The law does not apply to voiceprint data retained by a financial institution or an affiliate of a financial institution as defined by 15 U.S.C. § 6809. Unlike BIPA, there are no other statutorily identified exclusions to the definition of biometric identifier.

The key limitation of CUBI is that it only applies to biometric identifiers that are captured for a commercial purpose, but does not define commercial purpose. Unlike Washington's law, CUBI does not specifically exclude from coverage a biometric identifier collected by an employer for security purposes. This suggests that its scope is broader than Washington's law and that those biometric identifiers may be covered (Tex. Bus. & Com. Code Ann. § 503.001(c)(3)(c-2)).

Washington's law defines biometric identifier as data generated by automatic measurements of an individual's biological characteristics, such as:

- A fingerprint.
- A voiceprint.
- Eye retinas.
- Irises.
- Other unique biological patterns or characteristics used to identify a specific individual.

The statute specifically excludes from the definition of biometric identifier:

- Physical or digital photographs.
- Video or audio recordings or data generated from video or audio recordings.
- Information collected, used, or stored for health care treatment, payment, or operations under HIPAA.

(RCW 19.375.010(1).)

Similar to CUBI, Washington's law only applies to biometric identifiers enrolled in a database or collected or used for a commercial purpose. However, the Washington law specifically defines commercial purpose and limits its scope by:

- Requiring the sale or disclosure to a third party for the purpose of marketing goods or services that are unrelated to the initial transaction in which the person obtained the biometric identifier.
- Excluding from coverage data collected for a security purpose or law enforcement purpose.

(RCW 19.375.010(4), (8); 19.375.020(7).)

Washington's law does not apply to the disclosure or retention of biometric identifiers that:

- Have been unenrolled.
- Are used for a security purpose, defined as:
  - preventing shoplifting, fraud, or other misappropriation or theft; and
  - other purposes to protect the security or integrity of software, accounts, applications, online services, or any person.

(RCW 19.375.020(6), (7); 19.375.010(8).)

Notice and Consent

Illinois has the most onerous and specific notice requirements. Under BIPA, before an employer collects, captures, or otherwise obtains its employees' biometric identifiers or biometric information for any reason, it must first:

- Provide written notice to each employee that a biometric identifier or biometric information is being collected, including:
  - the specific reason for the collection, storage, and use; and
  - how long the employer will use or retain the biometric identifier or biometric information.
- Receive the employee's written release for the biometric collection signed by the employee as a condition of employment.
- Develop a publicly available written policy that includes:
  - a retention schedule; and
  - guidelines for the permanent destruction of the biometric information when the initial purpose for which it was collected no longer exists or within three years of the employee's last interaction with the employer, whichever is earlier.

(740 ILCS 14/15(a), (b); 14/10.)

Under CUBI, an employer cannot capture an employee's biometric identifier for a commercial purpose unless the employer:

- Informs the employee before capturing the biometric identifier.
- Receives the employee's consent to capture the biometric identifier.

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

Unlike BIPA, however, CUBI:

- Only applies to biometrics captured for a commercial purpose, though it does not define commercial purpose.
- Does not require that the notice or consent be in writing or in any particular form.

Washington's law is less restrictive than BIPA, but provides greater clarity than either BIPA or CUBI. Covered persons in

Washington cannot enroll a biometric identifier in a database for a commercial purpose without first doing one of the following:

- Providing notice.
- Obtaining consent.
- Providing a mechanism to prevent the later use of a biometric identifier for a commercial purpose.

(RCW 19.375.020(1).)

Notice is specifically defined as a disclosure reasonably designed to be readily available to the affected persons. Washington's law expressly states, however, that the appropriate form or type of notice or consent depends on the context. Unlike BIPA, but similar to CUBI, there is no specific requirement that notice be in writing.

(RCW 19.375.020(2).)

Restrictions on Sale, Use, and Disclosure

Under BIPA, private entities must not sell, lease, trade, or otherwise profit from an employee's biometric identifier or biometric information under any circumstances (740 ILCS 14/15(c)). BIPA also imposes strict requirements regarding the use and disclosure of biometric information. For example, BIPA prohibits covered entities from disclosing, redisclosing, or otherwise disseminating an employee's biometric identifier or biometric information, unless:

- The employee (or the employee's legal representative) consents to the disclosure or redisclosure.
- The disclosure or redisclosure completes a financial transaction that the employee (or the employee's legal representative) authorized.
- Federal, state, or local law requires the disclosure or redisclosure.
- The disclosure is required under a valid warrant or subpoena.

(740 ILCS 14/15(d).)

The restrictions on selling and disclosing biometric information also apply to third parties that maintain or manage databases that consist of employees' (or other individuals') biometric information, such as professional employer organizations (PEOs), staffing companies, or payroll service providers, and any third parties that maintain or manage the security systems that use, collect, or store biometric information.

Under CUBI, an employer that possesses a biometric identifier captured for a commercial purpose of an employee may not sell, lease, or otherwise disclose it to another person unless:

- The employee consents to the disclosure for identification purposes in the event of the employee's disappearance or death.
- The disclosure completes a financial transaction that the employee requested or authorized.
- The disclosure is required or permitted by a federal or state statute other than the Texas open government provision in Chapter 552 of the Texas Government Code (Tex. Gov't Code Ann. §§ 552.001 to 552.353).
- The disclosure is made by or to a law enforcement agency for a law enforcement purpose in response to a warrant.

(Tex. Bus. & Com. Code Ann. § 503.001(c)(1).)

Unlike BIPA, there is no outright ban on the sale of biometric information, provided other requirements for disclosure are met. In addition, there is no specific language required for notice or consent, or any requirement that the consent be in writing.

Under Washington's law, an employer that has enrolled an employee's biometric identifier may not sell, lease, or disclose it to another person for a commercial purpose unless either:

- The employer obtains the employee's consent.
- The sale, lease, or disclosure is:
  - consistent with the law's requirements;
  - necessary to provide a product or service subscribed to, required by, or expressly authorized by the employee;
  - necessary to effect, administer, enforce, or complete a financial transaction that the employee requested, initiated, or authorized, and the third-party recipient of the biometric identifier maintains its confidentiality and does not further disclose it;
  - required or expressly authorized by statute or court order;
  - made to a third party that contractually promises not to disclose it or enroll it in a database for a commercial purpose inconsistent with the law; or
  - made in preparation for litigation or to respond or participate in judicial process.

(RCW 19.375.020(3).)

Employers cannot use biometric identifiers in a way that is materially inconsistent with the initial purpose for which they were collected without obtaining new consent or providing a new disclosure (RCW 19.375.020(5)).

Although there is no case law interpreting Washington's law, common employer uses of biometric information may be excluded from coverage under the statute or fall within one or more of these exceptions. For example, fingerprints or retina scans that are collected and used for internal timekeeping data may not be considered as being used for a commercial purpose and therefore beyond the scope of coverage.

To the extent biometric information is used to prevent employees from being paid for time they have not worked, it also may be considered to be used for a security purpose. A security purpose includes the prevention of shoplifting, fraud, or any other misappropriation or theft of something of value, including tangible and intangible goods and services, and beyond the scope of coverage. (RCW 19.375.010(8); 19.375.020(7).) Similarly, information collected from a biometric timeclock that is shared with a PEO under an agreement to provide payroll services may fall within an enumerated exemption if the PEO agrees not to further disclose it or enroll it in a database for a commercial purpose (RCW 19.375.020(3)(e)).

Storage, Retention, and Destruction

Under BIPA, employers that possess biometric identifiers or biometric information must store, transmit, and protect the identifiers and information:

- Using the reasonable standard of care within the employer's industry (740 ILCS 14/15(e)(1)).

BEST PRACTICES FOR EMPLOYERS THAT COLLECT AND USE BIOMETRIC INFORMATION

Employers in every jurisdiction should:

- Be aware of the relevant biometric privacy laws, protections, and penalties for violating them in the jurisdictions where they have business operations and employ workers.
- Determine if they are collecting, using, storing, or transmitting any employee's (or other individual's) biometric identifiers or biometric information that may be covered by a biometric privacy statute, such as BIPA. This is important even if that information is not expressly cited in the statute or the use of the biometric identifier is not specifically required by the employer, such as an employee's use of an optional fingerprint recognition technology to access a company-issued smartphone.
- Determine what, if any, obligations they have regarding employee notice and consent, and other aspects of the use, storage, or destruction of biometric information.

Employers may want to proactively develop policies and practices that draw from BIPA's requirements, as BIPA is currently the most restrictive law addressing this issue (though depending on proposed amendments, this may change). If any biometric identifiers or biometric information is collected, used, stored, or transmitted, employers should also consider:

- Developing or reviewing existing written policies regarding the collection, storage, use, transmission, and destruction of biometric information, consistent with standards in the employer's industry.
- Implementing policies that provide proper notice to employees about the employer's collection, use, storage, and destruction of biometric information.
- Obtaining written and signed consent forms from all affected persons (as required in Illinois). Employers that routinely collect biometric information from all employees, such as those that use fingerprinting for timekeeping or retina scans to control building access, should consider making the employee's consent a condition of employment, either as part of an offer letter (that the employee signs to accept and commence employment) or in other onboarding materials.
- If the employer shares biometric information with any third party (such as a PEO or payroll service provider):
  - ensuring that the signed authorization (if used or required) addresses the employer's ability to share the biometric information with these business partners; and
  - requiring that the third party indemnify the employer for any damages resulting from the improper use, storage, or disposal of the biometric information by the third party.
- Establishing practices to protect employees' privacy against improper disclosure of biometric identifiers and biometric information using the same or more protective methods and standards of care that they use for other confidential and sensitive information.
- Notifying union representatives (if any) of any intent to collect or use a system that collects biometric information and preparing to bargain with the union over new practices if required by the collective bargaining agreement.
- Creating policies to respond to requests for accommodation from those employees who refuse to use the technology (for example, because of a religious belief) or are unable to use it (for example, because of an injury).
- Creating a response procedure and communication protocol in the event of a data breach.

Employers also should continue to monitor developments in this area, especially given the broad interpretations of BIPA's mandates to date.

- In the same (or a more protective) way that the employer stores, transmits, and protects other confidential and sensitive information (740 ILCS 14/15(e)(2)).

BIPA defines confidential and sensitive information as personal information that can be used to uniquely identify an individual or an individual's account or property, such as:

- A genetic marker.
- Genetic testing information.
- A unique identifier number to locate an account or property.
- An account number.
- A PIN number.
- A pass code.
- A driver's license number.
- A social security number.

(740 ILCS 14/10.)

Like BIPA, CUBI requires employers to use reasonable care in storing, transmitting, and protecting biometric identifiers from disclosure. Reasonable care means treating biometric identifiers the same as or in a more protective manner than the employer treats other confidential information. (Tex. Bus. & Com. Code Ann. § 503.001(c)(2).)

BIPA is the only state statute that currently allows for a private cause of action. This explains the disproportionate litigation brought under BIPA compared to the other biometric privacy statutes.

An employer that possesses an employee's biometric identifier must destroy the biometric identifier in a reasonable time, but no later than one year after the purpose for collecting the biometric identifier ends. In the case of a biometric identifier collected by an employer for security purposes, the purpose is presumed to expire when the employment relationship ends. (Tex. Bus. & Com. Code Ann. § 503.001(c)(2), (c)(3), (c-2).)

The retention requirements under Washington's law are similar to those under BIPA and CUBI. An employer that knowingly possesses a biometric identifier covered by the statute must:

- Use reasonable care to protect against its unauthorized access or acquisition.
- Not retain it longer than is reasonably necessary to:
  - comply with a court order, statute, or public records retention schedule;
  - protect against fraud, criminal activity, and other liability; or
  - provide the services for which the biometric identifier was enrolled.

(RCW 19.375.020(4)(a), (b).)

Remedies

BIPA is the only state statute that currently allows for a private cause of action. This explains the disproportionate litigation brought under BIPA compared to the other biometric privacy statutes. Under BIPA, a "person aggrieved" (which is not defined) can recover the greater of:

- For each negligent violation, the greater of:
  - liquidated damages of $1,000; or
  - actual damages.
- For each intentional violation, the greater of:
  - liquidated damages of $5,000; or
  - actual damages.
- Reasonable attorneys' fees and costs.
- Injunctive or other appropriate relief.

(740 ILCS 14/20.)

Although much of CUBI is modeled after BIPA, there is no private right of action under CUBI. Only the state attorney general can bring an action for violations of CUBI. Nonetheless, there is significant potential exposure for statutory violations of CUBI, including civil penalties of up to $25,000 for each violation (Tex. Bus. & Com. Code Ann. § 503.001(d)).

Similar to CUBI, there is no private right of action under Washington's law. It potentially creates, however, the greatest monetary exposure. Washington's law provides for the same remedies available for an unfair or deceptive act or method of competition, which carries with it civil penalties of up to $500,000. (RCW 19.375.030, 19.86.140.)

ADDITIONAL LAWS AFFECTING BIOMETRIC INFORMATION

Although only three states have enacted specific statutes addressing biometrics, many states regulate some aspect of biometric information in other ways. For example:

- Colorado requires that employers develop policies to properly dispose of paper documents containing personal identifying information, which is defined to include biometric data (C.R.S. § 6-1-713(1), (2)).
- Certain states include an individual's unique biometric data in the definition of "personal information" found in their general data breach notification statutes (see, for example, Iowa Code § 715C.1(11); Neb. Rev. Stat. §§ 87-802(5); Wis. Stat. § 134.98(1)(b)).
- The California Labor Code makes it a misdemeanor for an employer to require an employee or applicant to be photographed or 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 (Cal. Lab. Code § 1051).
- New York generally prohibits employers from fingerprinting applicants or employees as a condition of employment or continued employment unless specifically authorized by another law (N.Y. Lab. Law § 201-a).
- The North Carolina Identity Theft Protection Act lists biometric data as an element of identifying information that, if used with a person's name, constitutes personal information (N.C.G.S. §§ 75-61(10), 14-113.20(b)). Wyoming similarly includes biometric data as a data element that, if used with a person's name, constitutes personal identifying information (Wyo. Stat. Ann. §§ 40-12-501, 6-3-901(b)(xiii)).
- Florida prohibits public schools from collecting, obtaining, or retaining from students, or their siblings or parents, any biometric information, defined as information collected from

the electronic measurement or evaluation of any physical or behavioral characteristics attributable to a single person, including fingerprint, hand, eye, or vocal characteristics, and any other physical characteristics used to electronically identify a person with a high degree of certainty (§ 1002.222(1)(a), Fla. Stat.).

PROPOSED LEGISLATION

States that have proposed or considered biometric privacy laws include:

- Alaska.
- Connecticut.
- Massachusetts.
- Montana.
- New Hampshire.

Many of the bills have stalled in committee or died, potentially due in part to the rigorous lobbying efforts of companies against these laws. It remains to be seen whether biometric laws will become the next "paid sick leave" or "minimum wage" phenomena creating a patchwork of often conflicting state (and possibly local) laws posing challenges for multi-jurisdictional employers. However, given the increasing use of biometrics in HR functions, and the potential harm to employees if biometric information is compromised, more regulations are likely.

Significantly, an Illinois bill was introduced on February 15, 2018, that would create broad exemptions to BIPA (S.B. 3053, 100th Gen. Assemb. (Ill. 2018)). The proposed legislation would amend BIPA so that it would not apply to the use of biometric information if:

- The biometric information is used exclusively for:
  - employment;
  - HR;
  - fraud prevention; or
  - security purposes.
- The private entity does not sell, lease, trade, or similarly profit from the biometric identifier or biometric information collected.
- The private entity stores, transmits, and protects the biometric identifiers and biometric information in the same, or a more protective, way as it treats other confidential and sensitive information.

Amendments have been proposed to S.B. 3053 that would further narrow BIPA and the right to bring private causes of action under BIPA.

LITIGATION TRENDS AND DEVELOPMENTS

Employers should be aware of recent trends and developments in biometrics litigation, including:

- Consumer litigation that may inform BIPA pleading requirements.
- Cases addressing whether an employer's use of biometrics interferes with the employee's religious freedom.
- Cases discussing an employer's duty to subject new biometric processes to bargaining with a union.

CONSUMER LITIGATION

Although not arising in the employment context, recent consumer litigation under BIPA may be instructive to employers faced with claims for violating BIPA or other privacy statutes. One key issue that has been heavily litigated is whether mere violations of the statutory requirements are sufficient to state a claim under BIPA, or whether a plaintiff must plead and prove actual damages resulting from the violations.

Actual Damages Not Required

In *Sekura v. Krishna Schaumberg Tan, Inc.*, an Illinois state trial court held that a person need not plead actual damages to be a person aggrieved under BIPA. In this case, a tanning salon required its customers to scan their fingerprints as part of their membership for identification purposes. The plaintiff brought a class action claiming that the salon failed to provide sufficient notice about its use of the fingerprint data and properly safeguard it in violation of BIPA. The court relied on the plain language of the statute in concluding that any person whose biometric information was mishandled has a claim under the statute. (2017 WL 1181420, at *1-3 (Ill. Cir. Ct. Feb. 9, 2017).)

A federal district court in Illinois reached the same conclusion in *Monroy v. Shutterfly, Inc.* In that case the court relied on the statutory language regarding remedies and found that because the statute allows an aggrieved party to recover either liquidated damages or actual damages, a plaintiff need not prove actual damages to recover for a violation of the statute. (2017 WL 4099846, at *8-9.)

The US District Court for the Northern District of California reached the same result, holding that social media website users had standing to allege BIPA violations based on the collection of their biometric information, even absent allegations of any additional harm. The court found that by codifying a private right of action, the Illinois legislature indicated that procedural violations of the statute would cause concrete harm sufficient to confer Article III standing on litigants. (*Patel v. Facebook Inc.*, 2018 WL 1050154 (N.D. Cal. Feb. 26, 2018).)

Actual Damages Required

Several courts have held that individuals must suffer actual harm (as opposed to a mere technical violation) to bring an action under BIPA. For example, some courts have made this determination based on their interpretation of what it means to be a person aggrieved under BIPA (*Rosenbach v. Six Flags Entm't Corp.*, 2017 IL App (2d) 170317 (Ill. App. Ct. Dec. 21, 2017)).

Federal courts also have held that a plaintiff must plead actual damages to confer Article III standing (limiting federal court jurisdiction to "cases" and "controversies"). For example, in *Santana v. Take-Two Interactive Software, Inc.*, the US Court of Appeals for the Second Circuit dismissed the consumer plaintiffs' claims alleging that a gaming application's collection of biometric information by taking a face scan violated BIPA's notice and consent provisions. Despite allegations of technical violations of BIPA, the Second Circuit found that the plaintiffs

could not demonstrate an actual or imminent injury. Absent jurisdiction over the claims, the Second Circuit remanded to the district court to dismiss the case without prejudice. (2017 WL 5592589, at *3 (2d Cir. Nov. 21, 2017); see also *McCollough v. Smarte Carte, Inc.*, 2016 WL 4077108 (N.D. Ill. Aug. 1, 2016) (dismissing for lack of Article III standing plaintiff's claim for BIPA violations based on defendant's use of her fingerprint to lock and unlock a rented locker).)

Although the issue has not been definitively resolved, employers defending BIPA claims based solely on technical violations of the statute, such as the failure to provide adequate notice or obtain written consent, should consider bringing early motions to dismiss, especially for cases brought in federal court.

INTERFERENCE WITH RELIGIOUS BELIEFS

Several recent cases have raised the issue of whether an employer's (or other entity's) capture or use of an individual's biometrics interferes with the individual's religious freedom.

Several recent cases have raised the issue of whether an employer's (or other entity's) capture or use of an individual's biometrics interferes with the individual's religious freedom.

For example, in *EEOC v. Consol Energy, Inc.*, the US Court of Appeals for the Fourth Circuit held that an employer failed to accommodate an employee's religious beliefs in violation of Title VII of the Civil Rights Act of 1964 (Title VII). The employee, a devout evangelical Christian, believed that using the employer's biometric hand scanner (required for timekeeping) would associate him with the "Mark of the Beast," which brands followers of the Antichrist, and was therefore prohibited by his religion.

The employer contended and offered proof from the hand scanner manufacturer that the scanner did not place any mark on the person and therefore would not violate his religious beliefs. The employer also offered that the employee could use his left hand without any religious conflict, as only the right hand was associated with the Mark of the Beast. The Fourth Circuit found this evidence insufficient, especially given that the employer had accommodated other employees who could not use the scanner because of injuries. It upheld a jury award of more than $400,000 in damages for this violation. (860 F.3d 131 (4th Cir. 2017).)

In *Beach v. Oklahoma Department of Public Safety*, the plaintiff sought an accommodation relieving her from having her photo or fingerprint taken as part of her driver's license renewal. She contended that her sincerely held religious beliefs forbid her from participating in a global-numbering identification system, using the number of man, and that participating would eternally condemn her. She believed that the biometric photo and fingerprint that the motor vehicles department required for license renewal was an identification system forbidden in the Bible. The plaintiff based this belief on the motor vehicles department's practice of taking measurements off facial points from the photo to determine and assign a number that is specific to her for use with facial recognition technology. The court ultimately found that the matter was moot because the plaintiff had previously submitted to photos and fingerprints. (398 P.3d 1, 6 (Okla. 2017).)

Employers should be mindful of these decisions when facing requests, as a religious accommodation, to be excused from using a biometric timeclock or other biometric applications. Employers should not judge the validity of the religious practice, but rather determine whether:

- The employee's religious beliefs are sincerely held.
- There is a reasonable accommodation available that does not pose an undue hardship.
- The employer has granted a similar accommodation for other reasons, such as for a disability.

Search Religious Discrimination and Accommodation Under Title VII for more on the federal law prohibiting discrimination, harassment, and retaliation against applicants and employees on the basis of religion.

DUTY TO BARGAIN WITH A UNION

Employers with a unionized workforce have a duty to bargain with the union when implementing certain changes to workplace processes or policies. Generally, an employer may not unilaterally impose material changes in terms or conditions of employment that are mandatory subjects of collective bargaining without first negotiating to impasse. Not every working condition change, however, is sufficiently material or significant to trigger the duty to bargain.

Search Collective Bargaining Under the National Labor Relations Act for more on collective bargaining obligations set by the National Labor Relations Act and enforced by the National Labor Relations Board.

In several cases, employees have challenged an employer's installation of biometric timeclocks without bargaining about the issue. For example, in *Res Care, Inc.*, the employer had used a manual timekeeping system to record employee hours worked. The employer unilaterally, without bargaining, changed its timekeeping procedures by adding a biometric (fingerprint) timekeeping system. The employer also unilaterally added a weekly timesheet submission policy that required employees to sign in and out of work by placing their fingers on a sensor. The sensor scanned the employees' fingerprints and recorded their hours of work.

The administrative law judge (ALJ) found that this was not a material change that required bargaining because employees were already required to accurately record their time. (2001 WL 1598700 (N.L.R.B. Div. of Judges June 8, 2001) (new system did not involve more supervisory oversight of employees, but merely changed how the employer managed an existing requirement); see also *Rust Craft Broad. of N.Y., Inc.*, 225 N.L.R.B. No. 65 (1976) (change in practice of how time was recorded did not change the rule requiring that employees record their time).)

However, in another case, the ALJ found that implementing a new biometric timeclock, combined with requiring for the first time that employees record their time, scan in and out up to four times per day, and confirm their time reports, was a substantial and material matter that required the employer to bargain with the union (*Spartan Aviation Indus., Inc.*, 2011 WL 2412622 (N.L.R.B. Div. of Judges June 9, 2011)).

Employers with a unionized workforce should carefully review their collective bargaining agreements and analyze the facts of each case to determine whether any new timekeeping requirements or other biometric processes are subject to mandatory bargaining.