Expert Q&A on Biometrics in the Workplace: Recent Developments and Trends

PRACTICAL LAW LABOR & EMPLOYMENT

Search the Resource ID numbers in blue on Westlaw for more.

An Expert Q&A with Susan Gross Sholinsky and Peter A. Steinmeyer of Epstein Becker Green on the collection and use of biometric data in the workplace. It includes a definition of biometrics and covers the impact of recent class actions under the Illinois Biometric Information Privacy Act (BIPA), other state legislation regulating biometric data, and current trends in the usage and protection of employees' biometric data.

Employers nationwide are increasingly using biometric data for authentication, security purposes, and recording employee worktime. Presently, no comprehensive federal law specifically addresses an employer's obligations regarding the use or disclosure of its employees' biometric data. However, some states have passed laws regulating these activities in the employment context. A spate of recent class action lawsuits under the Illinois Biometric Information Privacy Act (BIPA) and a new biometric privacy law in Washington state has brought this issue to the forefront for employers that collect and use this data and may signal litigation and legislative trends going forward.

Practical Law Labor & Employment reached out to Susan Gross Sholinsky and Peter A. Steinmeyer of Epstein Becker Green for their insights on the existing laws in various jurisdictions, what employers should do to comply with them, and how to prepare for likely future developments in this area.

Susan is a Member of the Firm in the Employment, Labor & Workforce Management practice. She practices in the Firm's New York office, where she advises employers on all facets of the employment relationship, from pre-employment considerations and hiring to terminations and post-employment restrictions. She counsels clients in a practical and straightforward manner, with an eye toward reducing the possibility of employment-related claims. She also serves on the adjunct faculty of the Cornell University School of Industrial and Labor Relations, where she teaches courses concerning human resources and the law. She frequently speaks at events and webinars on employment law topics and authors numerous publications on employment law issues.

Peter is a Member of the Firm in the Employment, Labor & Workforce Management practice, the Chicago office Managing Shareholder, and a member of the Firm's Board of Directors. Practicing all aspects of labor and employment law, he has extensive experience litigating employment-related cases in numerous industries. Among other professional accolades, Peter received an "AV Preeminent" Peer Review Rating by Martindale-Hubbell and was named to the Illinois Super Lawyers list (2006 to 2017) in the area of Employment & Labor. Peter also regularly teaches seminars and speaks on a broad range of issues involving the workplace, has been quoted in many publications, and is an editor of the Firm's Trade Secrets & Noncompete Blog.

WHAT IS BIOMETRICS?

Although there is no universally accepted definition, 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 those characteristics.

Biometric identifiers are data generated by automatic measurements of an individual's biological characteristics. Biometric data or information is information derived from biometric identifiers.

Although statutory definitions vary, biometric identifiers may include:

- Retina or iris scans.
- Fingerprints.
- Voiceprints.
- Scans or records of hand or face geometry.
- 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.

However, it is unclear whether photographs (or information derived from photographs) are considered to be biometric identifiers. At least one court has found that a digital image of an individual's face geometry could be considered a biometric identifier (*In re Facebook Biometric Info. Privacy Litig.*, 185 F. Supp. 3d 1155, 1171 (N.D. Cal. 2016)).

WHAT IS UNIQUE ABOUT BIOMETRIC DATA?

Biometric data is different from other personally identifying information collected from employees. Unlike other information, such as a social security number, which can be changed if compromised, employees cannot change their biometrics. As the Illinois statute (BIPA) explains, biometric data is "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 may warrant greater protections (and penalties for violating those protections) than misuse or theft of other personal information.

HOW DO EMPLOYERS USE BIOMETRIC DATA?

Employers have been using biometric information with increasing frequency for various human resource and business functions. Common uses by employers include:

- Timekeeping, such as using fingerprints or hand scans to punch in and out on biometric timeclocks.
- Electronic security and building access, such as 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, such as computer systems, copiers, and applications on laptops, tablets, and smartphones, using facial recognition or fingerprinting technology.

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

WHAT LEGAL OBLIGATIONS DO EMPLOYERS HAVE WHEN COLLECTING, USING, STORING, OR DESTROYING EMPLOYEES' BIOMETRIC DATA?

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

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

Other states have been considering similar legislation. While the existing and proposed statutory requirements and restrictions differ, common themes include:

- Requiring some form of notice that the data is being collected and explaining 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 data.
- Providing standards for confidentiality, retention, and data disposal when the data is no longer needed for any purpose for which it was collected.

ILLINOIS

The Illinois BIPA, which has been in effect since 2008, imposes the most onerous restrictions and requirements on employers regarding the collection, use, storage, disposal, and disclosure of biometric data. BIPA applies to all private entities and is not limited to activities done for a commercial purpose.

BIPA defines biometric identifier as a:

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

(740 ILCS 14/10.)

The definition specifically excludes, among others:

- Writing samples and written signatures.
- Photographs.
- Biological samples, organs, and tissues.
- Biological materials regulated under the Illinois Genetic Information Privacy Act.
- Information collected in a health care setting or collected or used for health care treatment.

(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).

Under BIPA, before an employer collects biometric identifiers or information from its employees, it must:

- Provide written notice to each employee whose data is being collected that includes:
  - the reason for the collection; and
  - how long the employer will use or retain it.
- 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
  - destruction procedures.

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

Employers must safeguard biometric data in the same (or a more protective) way that they protect other confidential information using a reasonable standard of care (740 ILCS 14/15(e)). BIPA also expressly prohibits private entities from:

- Selling, leasing, or otherwise profiting from an individual's biometric data under any circumstances (740 ILCS 14/15(c)).
- Disclosing or redisclosing an individual's biometric data, unless:
  - the individual consents to the disclosure;
  - the disclosure completes a financial transaction that the individual authorized;
  - federal, state, or local law requires the disclosure; or
  - the disclosure is authorized by a 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 data, such as PEOs, staffing companies, or payroll service providers, and any third parties that maintain or manage the security systems that use, collect, or store this information.

TEXAS

The Texas law (CUBI) has been in effect since 2009 and is similar to BIPA, with a few variations. In Texas, 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).)

The definition of a biometric identifier is essentially the same as under BIPA (Tex. Bus. & Com. Code Ann. § 503.001(a)).

An employer that possesses a biometric identifier of an employee captured for a commercial purpose cannot 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).)

An employer that possesses an employee's biometric identifier must destroy the biometric identifier within a reasonable time but no later than one year after the purpose for collecting the identifier ends. If an employer collects a biometric identifier 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 Texas law differs from BIPA in several ways, including that the Texas law:

- Only applies to the capture of biometric identifiers for a commercial purpose, though commercial purpose is not defined. BIPA does not contain this limitation. Absent further guidance, employers should assume that data gathered to assist them in running their businesses efficiently and accurately paying their employees may constitute a commercial purpose under the law. The law specifically recognizes that biometric identifiers may be collected "for security purposes by an employer" (Tex. Bus. & Com. Code Ann. § 503.001(c)(3), (c-2)).
- Does not provide specific requirements for notice or consent or require that notice be in writing.
- Does not ban outright the sale of biometric data, provided other requirements for disclosure are met.
- Contains no private right of action.

WASHINGTON

In effect for less than a year, Washington state's law contains some significant limitations on the definition of biometric data, perhaps in response to the flurry of litigation under BIPA. For example, its definition of biometric identifier specifically excludes "physical or digital photographs" (RCW 19.375.010(1)). In addition, the notice and consent requirements also less onerous and more flexible than in the other states' laws. The Washington law provides that "[t]the exact notice and type of consent required . . . is context-dependent" (RCW 19.375.020(1), (2)).

However, the biggest distinction may be that Washington's law only applies to biometric identifiers enrolled in a database or collected or used for a "commercial purpose." As defined, a commercial purpose:

- Requires the sale or disclosure to a third party.
- Excludes data collected for a security or law enforcement purpose.

(RCW 19.375.010(4).)

Although there is no case law interpreting this statute, common employer uses of biometric data may 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 under the statutory definition. To the extent this data is used to prevent employees from being paid for time they have not worked, it also may be considered data used for a security purpose, which includes the prevention of shoplifting, fraud, or any other misappropriation or theft of something of value, including tangible and intangible goods and services (RCW 19.375.010(8)).

WHAT REMEDIES ARE AVAILABLE FOR VIOLATIONS OF THESE LAWS?

At present, the Illinois BIPA is the only state statute with a private right of action. This explains in part the rash of class action lawsuits recently brought under BIPA.

In Illinois, under BIPA, an "aggrieved person" can recover the greater of:

- $1,000 or actual damages for each negligent violation.
- $5,000 or actual damages for each intentional violation.

- Attorneys' fees and costs.
- Injunctive relief.

(740 ILCS 14/20.)

In contrast, there is no private right of action in Texas or Washington, where only the state attorneys general can bring an action. Nonetheless, there is significant potential exposure for statutory violations of CUBI in Texas, with civil penalties of up to $25,000 for each violation (Tex. Bus. & Com. Code Ann. § 503.001(d)). Penalties in Washington are even harsher and can reach $500,000 (RCW 19.86.140).

DO ANY STATE LAWS ADDRESS BIOMETRIC DATA FROM ANOTHER ANGLE?

Although only three states have statutes specifically addressing biometrics, many states regulate some aspect of biometric data 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)).
- In California, it is 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
  - 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).
- Other states include biometric data in the definition of "personal information" found in their general data breach notification statutes, for example:
  - Iowa Code Sections 715C.1 to 715C.2;
  - Neb. Rev. Stat. Sections 87-802 to 87-806;
  - Wis. Stat. Section 134.98; and
  - Wyo. Stat. Ann. Sections 40-12-501 to 40-12-502.

WHAT ARE THE KEY TAKEAWAYS FOR EMPLOYERS FROM THE BIPA CASES SO FAR?

While the recent class action lawsuits do not all arise in the employment context, the courts have broadly interpreted BIPA's provisions and individual protections. Claims in the employment context primarily have involved biometric time clocks that use fingerprint scans for clocking in and clocking out and include claims against major hotel groups, restaurant chains, and airlines.

The most common allegations are that employers are unlawfully collecting and storing employees' fingerprints for timekeeping purposes without properly notifying the employees or obtaining their written consent. For this reason, employers in Illinois that collect or use biometric information must ensure compliance with BIPA's notice and consent procedures.

However, a recent BIPA case from the Second Appellate District in Illinois may lessen the practical effect and momentum of these cases. In *Rosenbach v. Six Flags Entertainment Corporation*, the court held that individuals must suffer actual harm (as opposed to a mere technical violation) to bring an action as a "person aggrieved" under BIPA (2017 IL App (2d) 170317 (Ill. App. Ct. 2017)). The US Court of Appeals for the Second Circuit reached a similar conclusion in *Santana v. Take-Two Interactive Software, Inc.* In that case, the plaintiffs alleged that the collection of biometric data by taking a face scan in a gaming application violated BIPA's notice and consent provisions. The court dismissed the action because the plaintiffs could not demonstrate a material risk of harm from the practice, despite technical violations of the statute. (2017 WL 5592589, at *3 (2d Cir. Nov. 21, 2017).)

DO YOU EXPECT OTHER STATES OR LOCAL JURISDICTIONS TO PASS LAWS GOVERNING EMPLOYERS' USE AND DISCLOSURE OF BIOMETRIC DATA?

The state of Washington was the most recent jurisdiction to pass a biometric privacy law. Laws have been proposed or considered in other jurisdictions, including Alaska, Connecticut, Massachusetts, Montana, and New Hampshire. It remains to be seen whether biometric laws will become the next paid sick leave 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 this data is compromised, more regulations in this arena are likely.

WHAT STEPS CAN EMPLOYERS IN ILLINOIS AND ELSEWHERE TAKE TO STAY AHEAD OF THE CLASS ACTION CURVE?

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 in fact they are collecting, using, storing, or transmitting any employee's (or other individual's) biometric information or identifiers that may be covered by a biometric privacy statute, such as BIPA.

This is important even if that data is not expressly cited in the statute or the use of the identifier is not specifically required by the company, such as an employee's use of an optional fingerprint recognition technology to access a company-issued smartphone.

If any biometric data or identifiers are collected, used, stored, or transmitted, employers in Illinois should:

- Develop or review existing written policies regarding the collection, storage, use, transmission, and destruction of that information, consistent with standards in the employer's industry.
- Implement policies concerning proper notice to their employees about the employer's collection, use, storage, and destruction of that information and obtain written and signed consent forms from all affected persons. Employers that routinely collect this 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 or in other onboarding materials.

- To the extent the employer shares biometric information with any third party (such as a PEO or payroll service provider), ensure that the signed authorization addresses the employer's ability to share the information with these business partners.
- Establish practices to protect individuals' privacy against improper disclosure of biometric data and identifiers using the same or more protective methods and standards of care that they use for other confidential and sensitive information.

Employers in Texas, Washington, and other states that regulate biometric data under related statutes should determine what, if any, obligations they have regarding employee notice and consent and other aspects of the use, storage, or destruction of this data. Employers in these and other jurisdictions that collect biometric data may want to proactively develop policies and practices similar to what is required under BIPA, as it is currently the most restrictive law addressing this issue.

Finally, employers should continue to monitor the fast-moving developments in this area, especially given the broad interpretations of BIPA's mandates to date.