EPSTEIN BECKER GREEN | Employment, Labor & Workforce Management

ACT NOW ADVISORY

Recent Surge in Class Actions Involving "Biometric" Data: What Employers Need to Know and Do *Now*

January 3, 2018

By Peter A. Steinmeyer, Susan Gross Sholinsky, and Michelle G. Marks

---

In the past six months alone, roughly 30 employment class actions have been filed in Illinois claiming violations of a state law that some employers may have never even heard of, or are only vaguely familiar with—the 2008 Biometric Information Privacy Act ("BIPA").[1] In short, BIPA protects the privacy rights of employees, customers, and others in Illinois against the improper collection, usage, storage, transmission, and destruction of biometric information, including biometric identifiers, such as retina or iris scans, fingerprints, voiceprints, and scans of face or hand geometry.

Employers nationwide are increasingly using biometric data for authentication, security purposes, and recording employee work time. However, the spate of recent lawsuits over how such information is being handled suggests that more than a few companies may not be aware of, or appreciate, their legal obligations in this arena. These obligations range from securing an individual's permission in advance of collecting his or her biometric information, to properly storing, and later disposing of, that data. For instance, many of the suits currently before the courts allege that employers are unlawfully collecting and storing employees' fingerprints for timekeeping purposes by failing to notify those employees that the information is being collected and stored, and by not obtaining a release from those employees authorizing them to do so.

Moreover, BIPA's reach extends beyond the employer-employee relationship. For example, one restaurant chain's use of customers' facial scans to confirm their orders at self-service stands is being challenged. Further, at least one court has applied BIPA to the use of biometric identifiers not specifically covered by the statute, and permitted a claim to proceed where the business used facial-recognition software on photographs—a biometric identifier not expressly included in BIPA.

Since BIPA's passage, biometric privacy laws were enacted in Texas (the Capture or Use of Biometric Identifier Act of 2009) and Washington State (its 2017 law governs the enrollment, disclosure, and retention of biometric identifiers). Colorado also regulates the disposal of this information by including biometric data in the definition of "personal

---

[1] 740 ILCS 14/1 *et seq.*

information." And Alaska, Connecticut, Montana, and New Hampshire are considering enacting laws similar to BIPA.[2]

Why Is Biometric Information Given Special Protection?

As BIPA itself explains, biometric information is unlike, say, Social Security numbers, which, if compromised, can be changed. Rather, biometric data is "biologically unique to the individual; therefore, once compromised, the individual has no recourse … [and] is at heightened risk for identity theft …" and other problems. Accordingly, BIPA broadly regulates "the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information."

BIPA's Requirements on the Collection, Usage, Storage, Disposal, and Disclosure of Biometric Data and on Notice and Consent

BIPA defines "biometric information" as "any information … based on an individual's biometric identifier used to identify an individual," regardless of how that information is captured, converted, stored, or shared.[3] The statute permits a "private entity" to collect, store, or use biometric identifiers and data from individuals, **only if it first:**

- *develops a written policy,* made available to the public, that includes a:
    - retention schedule;
    - retention guideline; and
    - process for permanently destroying biometric identifiers and information 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 private entity, whichever occurs first; and
- *provides notice to, and obtains consent from, each subject of collection.* Prior to collecting, capturing, purchasing, or otherwise obtaining a person's biometric identifier or information, the private entity must:
    - inform the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric data is being collected and stored;
    - advise the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

[2] It should be noted here that other states, such as New York, maintain laws that generally prohibit employers from requiring, as a condition of employment or continued employment, employees to be fingerprinted (except as may otherwise be required by law). *See, e.g.,* N.Y. Labor Law § 201-A.

[3] Generally, "biometric information" does not include writing samples, photographs, physical descriptions, or human biological samples used for medical or scientific purposes.

- obtain a *written release* signed by the subject or the subject's legally authorized representative of the biometric identifier or information.

Moreover, BIPA expressly prohibits private entities from:

- selling, leasing, or otherwise profiting from a person's biometric identifier/information; or

- disclosing or re-disclosing an individual's biometric identifier/information, *unless*:

  - the subject of the identifier/information consents to the disclosure;

  - the disclosure completes a financial transaction authorized by that individual;

  - the disclosure is required by federal, state, or local law; or

  - the disclosure is authorized pursuant to a warrant or subpoena.

These restrictions on selling/disclosing biometric information without proper consent or legal authorization also apply to third parties that maintain or manage databases that consist of employees' (or other individuals') biometric data and any third parties that maintain or manage the security systems that use, collect, or store such information.

"Standard of Care"

Private entities must use the "reasonable standard of care" applicable to their industry with respect to storing, transmitting, and protecting biometric identifiers and information from disclosure. Specifically, the manner in which such identifiers or data is stored, transmitted, and protected from disclosure must be the same as, or more protective than, the manner in which other "confidential and sensitive" information is so handled.

Penalties for Violations of BIPA

Any person who is "aggrieved by a violation" of BIPA and who can demonstrate that a private entity was *negligent* with respect to implementing a provision of BIPA may recover for each violation liquidated damages of $1,000 or actual damages, whichever is greater. If the private entity is found to have *intentionally* violated the statute, an aggrieved individual can recover for each violation liquidated damages of $5,000 or actual damages, whichever is greater. In the case of either a negligent or intentional violation, an aggrieved individual may also recover reasonable attorneys' fees and costs, and a court may grant the prevailing party injunctive relief. Courts are currently wrestling with whether an individual must make a showing of actual damages in order to state a claim under BIPA. But last week, an Illinois appellate court held that in order for any of the BIPA remedies to come into play, the plaintiff must be "aggrieved" by a violation of BIPA and, thus, must allege an actual injury or adverse effect, and not just a technical violation of the statute.

What Employers Should Do Now

First, employers with operations in Illinois should 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 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 employee use of optional fingerprint recognition technology to access a company-issued smartphone.

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

- develop or review existing, written policies concerning the collection, storage, use, transmission, and destruction of that information, consistent with industry standards;

- implement policies concerning proper notice to their employees (and other affected individuals) about the company's use, storage, etc., of such data and obtain written and signed consent forms from all affected persons; and

- establish practices to protect individuals' privacy against improper disclosure of biometric data/identifiers, using the methods and standard of care that they would apply to other material deemed confidential and sensitive.

Second, employers that collect, store, or use biometric identifiers or information in other jurisdictions, including Texas, Washington State, and Colorado, should determine if they may have legal obligations concerning such data in those venues.

Finally, employers should continue to monitor the fast-moving developments in this area, as the courts seem inclined to broadly interpret BIPA's mandates.

****

For more information about this Advisory, please contact:

Peter A. Steinmeyer	**Susan Gross Sholinsky**	**Michelle G. Marks**
Chicago	New York	Chicago
312-499-1417	212-351-4789	312-499-1440
psteinmeyer@ebglaw.com	sgross@ebglaw.com	mgmarks@ebglaw.com

About Epstein Becker Green

Epstein Becker & Green, P.C., is a national law firm with a primary focus on health care and life sciences; employment, labor, and workforce management; and litigation and business disputes. Founded in 1973 as an industry-focused firm, Epstein Becker Green has decades of experience serving clients in health care, financial services, retail, hospitality, and technology, among other industries, representing entities

from startups to Fortune 100 companies. Operating in offices throughout the U.S. and supporting clients in the U.S. and abroad, the firm's attorneys are committed to uncompromising client service and legal excellence. For more information, visit www.ebglaw.com.