BCLP. Client Intelligent

BCLPatWork.com

BIOMETRIC PRIVACY TARGETED IN INCREASED CLASS ACTION LITIGATION IN ILLINOIS

Nov 17, 2017

Even as technology advances and consumers become more accustomed to providing their fingerprints in routine, everyday transactions (such as unlocking their cellular phones), private entities, and employers in particular, are under attack in the courts for their use of finger-scan and biometric technology.

The Illinois Biometric Information Privacy Act ("BIPA"), effective since October 2008, regulates the collection, use, safeguarding, handling, storage, retention, destruction, and disclosure of biometric identifiers and information. The BIPA, however, was largely ignored until mid-2015 when the first wave of BIPA litigation was filed against social media and photo-storage/sharing services.

BIPA litigation has now turned its attention to employers. Since August 2017, in Cook County, Illinois alone, more than 30 class action lawsuits have been filed in state court alleging violations of the BIPA, mostly based on employers' use of finger-scan technology for timekeeping tracking. The recent lawsuits generally allege that employers have collected, stored, and/or used workers' fingerprints without providing notice to workers or obtaining consent. They also allege that employers lack written policies establishing a retention and destruction schedule for workers' biometric information or identifiers. It has not yet been determined whether such timekeeping practices violate the BIPA.

What is a biometric identifier? A "biometric identifier" under the BIPA is defined as:

- A retina scan
- An iris scan
- A fingerprint
- A voiceprint
- A scan of hand geometry
- A scan of face geometry

The BIPA expressly excludes the following from the definition of "biometric identifiers": writing samples; written signatures; photographs; human biological samples used for valid scientific testing or screening; demographic data; tattoo descriptions; physical descriptions; donated organs, tissues, parts, blood, or serum; and other images or films of human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

What is biometric information? Under BIPA, "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. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers."

What does the BIPA require? Generally, the BIPA imposes four central requirements on private entities possessing, collecting, capturing, purchasing, receiving, otherwise obtaining, or disclosing a person's biometric identifier or information.

First, the entity "must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information" and comply with the established retention schedule and destruction guidelines.

Second, the entity must inform a person (or a legally authorized representative) in writing that his/her biometric identifier or biometric information is being collected, stored, used, or disclosed and set forth the purpose and length of term for which a biometric identifier or biometric information is being collected.

Third, the entity must receive a written release consenting to the collection, use, storage, or disclose of biometric identifiers or biometric information.

Fourth, the entity in possession of a biometric identifier or biometric information must store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within that entity's industry and in a manner that is the same or more protective that the manner in which the entity stores, transmits, and protects other confidential and sensitive information.

What does the BIPA prohibit? The BIPA prohibits a private entity from selling, leasing, trading, or otherwise profiting from a person's biometric identifier or biometric information.

What are potential consequences of non-compliance with the BIPA? Illinois is the only biometric privacy law that provides "aggrieved" consumers or workers a private cause of action and allows persons to directly sue in court for alleged violations. No court, however, has determined what it means to be "aggrieved" under the BIPA. For each violation of the BIPA, a prevailing party may potentially recover: liquidated statutory damages of $1,000 (for negligent violations) or $5,000 (for intentional or reckless violations), or actual damages, whichever is greater. Attorneys' fees and

costs, including expert witness fees and other litigation expenses, may also be recoverable. Injunctive relief is also available where warranted. Given that BIPA lawsuits have been filed as class actions, exposure for companies in violation of the BIPA can potentially be significant.

Are there defenses to violations of the BIPA? Potential defenses to a BIPA claim include: (1) lack of "aggrievement"; (2) lack of standing; (3) substantial compliance with the BIPA; (4) release, consent, ratification, acquiescence; (5) laches or statute of limitations; (6) contributory or comparative negligence/last clear chance; (7) estoppel; (8) waiver; (9) good faith; and/or (10) unenforceability of liquidated damages without actual injury. Litigants have also challenged the constitutionality of the BIPA on due process grounds, asserting that the BIPA's statutory damages are grossly excessive and disproportionate without proof of actual injury. Defenses to jurisdiction, venue, and/or class certification should be explored at the outset of litigation.

What can companies do to assess their risk and reduce exposure? There have been numerous cases already filed related to the use of biometrics and extensive future litigation is anticipated. Companies using biometric technology should ensure they have a solid understanding of the technology being utilized and review their policies. Bryan Cave has extensive experience counseling and defending businesses in these areas.

The States of Washington and Texas also currently have biometric privacy laws affecting private employers or companies, but these do not provide for private rights of action. Other biometric privacy laws have previously been proposed in Nebraska, Iowa, North Carolina, Wisconsin, Oregon, Wyoming, California, and New York.

Additionally, for more information on fingerprint identification and facial recognition technology, please also see the following articles:

https://www.bryancave.com/en/thought-leadership/fingerprint-identification-technology-a-how-to-guide.html

https://www.bryancave.com/en/thought-leadership/facial-recognition-technology-a-how-to-guide.html

https://www.bryancave.com/en/thought-leadership/what-employers-should-consider-before-switching-to-fingerprint.html

Bryan Cave LLP has a team of knowledgeable lawyers and other professionals prepared to help employers assess their risk and reduce exposure to litigation. If you or your organization would like more information on biometric technology in the workplace or any other employment issue, please contact an attorney in the Labor and Employment practice group.

MEET THE TEAM

Mary Margaret (Mimi) Moore

Chicago / Dallas

mimi.moore@bclplaw.com
+1 312 602 5090

Lauren J. Caisman

Chicago

lauren.caisman@bclplaw.com
+1 312 602 5079

Jeffrey S. Russell

St. Louis

jeffrey.russell@bclplaw.com
+1 314 259 2725