Biometric Time Clocks May Be a Ticking Time Bomb for Employers

Authored by: Kevin D. Kelly and Brian I. Hays

Spring 2018

This article was reprinted with permission from the Spring 2018 issue of the Employee Relations Law Journal.

Employers in Illinois that are using biometric time clocks that use fingerprints or other biometric identifiers to identify particular employees need to be aware of the substantial compliance obligations imposed by the Illinois Biometric Information Privacy Act, 740 ILCS 14/1 et seq. ("BIPA" or the "Act"). Although the Act has been in place since 2008, it is just now garnering significant attention from class action plaintiffs' attorneys, with more than 30 class actions filed in 2017 alleging violations of the Act. The new wave of class actions focused on the use of biometrics in the workplace and the potentially significant penalties for violations of this Act mean that employers who have ignored the impact of this law need to take steps now to avoid problems in the future.

What is the Act and what does it require?

The Act applies to the collection and use of "biometric information," which is defined as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." A "biometric identifier" is "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."

The Act states that no entity may collect an individual's biometric identifier or biometric information unless it first:

- informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
- informs 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
- receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

Furthermore, an entity in possession of biometric identifiers or biometric information must develop a written policy "establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first."

As for penalties, the Act provides that an individual aggrieved by a negligent violation of the Act may recover, in a civil lawsuit, the greater of actual damages or liquidated damages of $1,000. For an intentional or reckless violation of the Act, an aggrieved individual can recover the greater of actual damages or liquidated damages of $5,000. In either case, an aggrieved individual can recover attorneys' fees and costs incurred in a successful lawsuit. An employer who has hundreds or thousands of employees using biometric time clocks or is capturing and using biometric information for other purposes (e.g., building access) faces the potential for very significant liability. Moreover, aggressive plaintiffs' attorneys may claim that the $1,000/$5,000 liquidated damage amounts apply not just per aggrieved person but to each and every violation of the law that occurs (such as each time someone uses a biometric time clock without having provided proper authorization for the collection and use of his or her biometric information).

Class Actions and Possible Defenses

Within the last 60 days, a number of class action lawsuits have been filed against employers over the use of fingerprints for timekeeping purposes. The plaintiffs in these cases contend that BIPA prohibits a company from collecting fingerprints without notifying the employees in writing that the information is being collected and obtaining written releases from the employees.

Defendants in BIPA cases have been challenging the plaintiffs' standing to bring BIPA claims. An individual who has not suffered a concrete injury lacks standing to file a lawsuit. *Spokeo v. Robins*, 136 S.Ct. 1540 (2016). Defendants have argued that plaintiffs have not been harmed by having their fingerprints or faces scanned absent some showing that the biometric information has been hacked. Defendants have also argued that the language in BIPA limiting the right to bring a cause of action to "[a]ny person ***aggrieved by*** a violation" the Act, requires a plaintiff to allege that he or she suffered actual damages from the violation. The courts are currently split on whether the collection of biometric information without more constitutes an injury in fact creating standing.

In *McCollough v. Smarte Carte, Inc.*, No. 16 C 03777, 2016 WL 4077108 (N.D. Ill. Aug. 1, 2016) and *Vigil v. Take-Two Interactive Software, Inc.*, 235 F. Supp. 3d 499 (S.D.N.Y. 2017), the courts granted motions to dismiss. In both cases, the defendants argued that the plaintiffs consented to the collection of their biometric information. In *McCollough,* the plaintiffs allowed their fingerprints to be scanned and used to open rental storage lockers. In *Vigil*, the plaintiffs sat in front of their game box for 15 minutes while their faces were scanned to created avatars for a video game. The courts found that because the plaintiffs had consented to the collection of the information, the failure to obtain a written release constituted a mere procedural violation that did not give rise to standing under *Spokeo.* The courts held that absent any allegation of a risk that the biometric information had been compromised, the collection of face and fingerprint scans did not constitute a concrete injury under *Spokeo.*

The court reached the opposite conclusion in *Monroy v. Shutterfly, Inc.*, 2017 WL 4099846 (N.D. Ill. Sept. 15, 2017). In Monroy, the plaintiffs alleged that they had no idea Shutterfly was collecting biometric information when the plaintiffs uploaded pictures to the Shutterfly website. The court found that the act of collecting biometric information without a person's knowledge constituted an invasion of privacy constituting a concrete injury.

An employer's collection of fingerprints for timekeeping purposes is much more akin to the scenarios in *McCollough* and *Vigil* than *Monroy.* Employees are fully aware that their fingerprints are being collected and that they will be used as part of the timekeeping system. However, employers should not rest easy. The *Vigil* case is currently on appeal to the Second Circuit Court of Appeals. Oral argument was heard on October 26, 2017. During oral argument, the parties agreed that collecting biometric information without the knowledge or consent of the individual would constitute a concrete injury giving rise to a claim under BIPA. The judges appeared to agree with the defendant that a plaintiff who knowingly allowed his or her biometric information to be collected must allege something more to have standing. The panel appeared to be struggling with the question of what a plaintiff has to allege to show harm from a risk of his or her biometric information being compromised. As long as the question of standing remains unresolved, employers using fingerprints for timekeeping face considerable exposure to suit.

Going Forward

In light of the potential for significant liability on a class-wide basis for violations of the Act, employers using biometric timeclocks or otherwise capturing and using biometric information in the workplace should consider whether these devices are worth the compliance headaches in the first place. Employers that wish to use or continue using these devices must ensure that they have a compliance program in place that meets all aspects of the Act, including, most importantly, the requirement of obtaining written consent from each individual before capturing that individual's biometric information. Employers with union workforces need to consider their potential obligation to bargain with the union over the implementation of biometric timeclocks or other use of biometric information in the workplace and also how to deal with employees who may, for whatever reason, refuse to consent to the collection of biometric information. Employers who do not comply with the Illinois Biometric Information Privacy Act can no longer fly "under the radar"— we can expect to see continued class action filings by aggressive plaintiffs' attorneys seeking to recoup maximum damages on a class-wide basis.

ABOUT THE AUTHORS

Kevin D. Kelly
Partner
Chicago
312-443-0217
kkelly@lockelord.com

Kevin Kelly is a partner in Locke Lord's Labor & Employment group. He helps clients solve labor and employment law problems with practical, cost-effective solutions.

Brian I. Hays
Partner
Chicago
312-443-1707
bhays@lockelord.com

Brian Hays focuses on defending clients in high stakes class action litigation. His practice includes the representation of insurance companies, financial institutions, and national corporations against claims brought under federal and state antitrust laws, RICO, the Telephone Consumer Protection Act, and other consumer protection statutes. He has participated in a wide variety of litigation matters before state and federal courts, including bench and jury trials.