LEGAL UPDATES PUBLISHED: OCTOBER 15, 2019

Overview of Recent Decisions Interpreting the Illinois Biometric Information Privacy Act

Services

Data Privacy & Cybersecurity

Labor & Employment

Professionals

ROBERT J. TOMASO
ST. LOUIS:
314.345.6433
BOB.TOMASO@
HUSCHBLACKWELL.COM

ANNE M. MAYETTE
CHICAGO:
312.341.9844
ANNE.MAYETTE@
HUSCHBLACKWELL.COM

Key Points

The Illinois Biometric Information Privacy Act (BIPA) is the most stringent privacy law in the country providing claimants with a private right of action without alleging actual injury.

Recent decisions have held that companies outside of Illinois that collect, store or use information on employees and persons in Illinois are subject to BIPA mandates.

Courts have held that notice of the collection of biometric information must be obtained from all persons prior to collection of the biometric information.

A recent decision acknowledged that an expansive reading of the statute suggests that each scan of biometric information may constitute a single violation under the BIPA.

Union employees subject to a collective bargaining agreement must pursue their BIPA claims in arbitration or before an administrative board.

Claims of willful or intentional violation of the new law must be supported by facts.

BIPA contains no statute of limitations for actions brought under the law, and the issue of the applicable length of the statute of limitations remains unresolved.

As tech companies race to develop facial recognition software for new applications across industry sectors, including the automotive, cosmetic, and healthcare industries, state legislatures are developing privacy laws to protect individuals' right to privacy and control over their biometric information. The Illinois BIPA is the most stringent biometric privacy law in the U.S for the following reasons:

It is the only biometrics privacy statute in the country with a private right of action that provides for liquidated damages for "aggrieved" parties" of up to $5,000 per violation.

The Illinois Supreme Court in *Rosenbach v. Six Flags Entertainment Corp.* (*Rosenbach*), which we discussed here, held that an individual need only prove a technical violation of BIPA and not actual damages to maintain a cause of action under it.

BIPA mandates that employers comply with collection, retention, disclosure and destruction protections prior to collecting biometric information as follows:
Notice of the collection, the purpose of retention, and storage of biometric information;
Acquisition of a written release from individuals to document consent to the collection, storage and use of the biometric information; and
Publication of document retention and destruction schedules of biometric information.

BIPA provisions forbid dissemination, trading, leasing, selling or otherwise profiting from biometric information.

BIPA, enacted in 2008, does not contain a statute of limitations on actions that may be brought.

BIPA has spawned numerous class action lawsuits for violation of privacy rights, including class actions against healthcare providers that used biometric authentication to protect confidential patient data and medications. Additionally, in the nine months following the *Rosenbach* decision, Illinois courts and the 9th U.S. Circuit Court of Appeals have released opinions on other issues raised by litigants. An overview of the opinions addressing those issues are discussed below.

Article III standing

In a decision of significant import, the 9th Circuit in *Patel v. Facebook Inc.*, held that plaintiffs in Illinois who alleged that Facebook's use of facial recognition technology used in photo tagging violated BIPA had alleged a concrete injury in fact to confer Article III standing. The 9th Circuit's decision concluded that Facebook's development of face templates using facial recognition technology without consent was the "very substantive harm targeted by BIPA," that BIPA protected concrete

privacy interests, and that plaintiffs alleged a concrete harm sufficient to confer Article III standing. The 9th Circuit further refused to decertify the class based on Facebook's extraterritorially argument. Instead, it upheld class certification because it concluded that it was reasonable to infer from General Assembly statements that the Illinois legislature contemplated application of BIPA to protect privacy interests of individuals located in Illinois even if some activities occurred in states other than Illinois. It also stated that if warranted by future circumstances, the district court could decertify the class.

The class alleged that Facebook collected and stored their facial images for tagging without prior notice and consent and without the required retention schedule in violation of BIPA provisions. Facebook moved to dismiss for lack of Article III standing, but a unanimous 9th Circuit upheld the district court decision that denied Facebook's motion.

The 9th Circuit decision is aligned with the *Rosenbach* decision, which held that the collection of biometric data without consent was sufficient to state a cause of action. These two decisions decisions are indicative of the courts' continued willingness to uphold the broad mandates of the statute.

Removal to federal court

Subject matter jurisdiction and diversity

In *Treadwell v. PowerSolutions Inc.* (*Treadwell*), the federal court refused to remand the case to state court after it was removed to federal court even though subsequent events resulted in a lack of diversity of jurisdiction between the parties.

In *Treadwell*, a plaintiff filed a class action complaint in state court alleging violations of BIPA against two defendant corporations. Defendants properly removed the case to federal court based on minimal diversity and satisfaction of the amount in controversy requirement. The plaintiff and the sole out-of-state defendant, NOVAtime, jointly stipulated to voluntary dismissal without prejudice. After dismissal of NOVAtime, the plaintiff filed a motion to remand the case to state court based on lack of subject matter jurisdiction in federal court as well as the home state or local exception to diversity jurisdiction under the Class Action Fairness Act (CAFA).

The Illinois court denied plaintiff's motion. When federal jurisdiction is proper at the time of removal, neither subsequent events nor the local exception affects the federal court's jurisdiction over the case.

Meaning of "each violation" and effect on amount in controversy requirement

In *Peatry v. Bimbo Bakeries USA, Inc.*, the court refused to narrowly interpret the term "each violation," which would have deprived the federal court of jurisdiction. In doing so, the court noted that plaintiff's "post removal attempt to cabin her damages so as to avoid federal court does not deprive the court of jurisdiction."

The plaintiff attempted to thwart defendant's subsequent removal of the case to federal court by claiming the amount in controversy for her individually and the class fell short of the jurisdictional threshold. Although plaintiff argued the definition of "each violation" was more limited, the pleadings indicated that she had scanned her fingerprint each time she clocked in and out of work, and that she was employed for thirty months. She also sought recovery of statutory damages of either $1,000 for each negligent violation of BIPA or $5,000 for each reckless or intentional violation. Additionally, the class was comprised of approximately 300 employees.

The court noted that the term "each violation" is undefined in BIPA and uninterpreted. Under an expansive reading of the statute, recovery of damages in excess of $5 million was plausible if counting each scan of an individual's fingerprint. The court denied plaintiff's motion to remand to state court because it was conceivable that she exceeded the amount in controversy requirement.

Although this issue remains unresolved, this case represents an indication that the term "each violation" can be defined broadly to refer to each scan and each disclosure to a third-party vendor rather than to each person whose biometric information was collected and shared. The prospect of a broad interpretation of the term continues to help fuel the filing of class action lawsuits.

Consent requires proper notice

In *Rogers v. CSX Intermodal Inc.* (*Rogers*), the court held that *Rosenbach* established that consent cannot be given by an individual unless there is proper notice that the biometric information will be collected, stored and used as required by the statute.

In *Rogers*, plaintiff claimed that he was entitled to recovery of damages under BIPA as a result of his employer's failure to disclose the purpose for which his fingerprint scans were collected, to disclose the length of time the information would be retained, and to obtain his consent to the collection and disclosure of the information to third-party vendors as required by BIPA. Defendant moved to dismiss the complaint arguing that BIPA allowed individuals to withhold consent *prior* to the collection of the biometric identifiers, asserting that an individual's right was not violated where the individual *voluntarily* scanned his or her fingerprints.

The court rejected defendant's argument because the Illinois Supreme Court had settled this issue in the *Rosenbach* decision. The court held that an individual's right to privacy encompasses the right to give up his biometric information *only after* receiving proper notice relating to the collection of the biometric identifiers and giving his or her consent to its collection. Further, like minors, adult individuals cannot consent voluntarily without receiving proper notice and providing written consent.

Arbitration of BIPA claims

Existence of a Collective Bargaining Agreement

In the consolidated cases *Miller v. Southwest Airlines Co. and Johnson v. United Airlines, Inc.*, the 7th Circuit held that plaintiffs, who were union workers subject to a collective bargaining agreement (CBA), must submit their claims under BIPA to the adjustment board under the Railway Labor Act.

Plaintiffs contended that the airlines implemented fingerprint scanning timekeeping systems and collected their fingerprints without their consent, failed to publish a public protocol for retaining and handling biometric data, and unlawfully disclosed the biometric data to third-party vendors. Defendants claimed the plaintiffs either expressly or through the CBA's management rights clauses received notice and consented to the collection and disclosure of the biometric data. Defendants also contended the claims must be submitted for arbitration to the adjustment board under the Railway Labor Act.

The 7th Circuit affirmed the lower court's dismissal of the suit *Miller v. Southwest Airlines Co.* in federal court because the method by which a union acquires and uses biometric data for timekeeping purposes constitutes a mandatory subject of collective bargaining reserved for resolution by the adjustment board under the Railway Labor Act.

The court similarly vacated and remanded the lower court's decision in *Johnson v. United Airlines, Inc.* with instructions to refer the parties' dispute to the adjustment board for the reason that the complaint concerned a CBA, which is regulated by federal law. Removal was also conceivably warranted under the CAFA.

Existence of mandatory arbitration provision in employment agreement

In *Liu v. Four Seasons Hotels Court*, the employer moved to compel arbitration of a BIPA lawsuit and claimed that the lawsuit constituted a wage and hour dispute because the issue was related to timekeeping. The employment agreement compelled arbitration for only four types of employment disputes, including wage and hours claims.

The court denied the motion because a cause of action under BIPA alleged a violation of privacy rights, not a wage and hour claim even though hotel employees' fingerprints were scanned and collected for the purpose of tracking hours worked. As such, the claims were not an arbitrable dispute under the employment agreement.

Claims of willful or reckless violations of BIPA

In *Rogers v. CSX Intermodal Inc.*, plaintiff alleged that defendant's actions were willful and wanton because CSX failed to take any steps to comply with BIPA mandates. The court disagreed.

A plaintiff must plead facts sufficient to support a claim of a willful or reckless violation of BIPA, and conclusory allegations are insufficient to overcome a motion to dismiss.

Constitutional defenses raised

In *Gregg Bruhn v. New Albertson's Inc.*, a class action suit alleged that the pharmacists' use of a fingerprint scanning system to access the pharmacy's computer system triggered the protections afforded under BIPA. Defendant filed a motion to dismiss arguing that the exclusion of certain financial and government entities from BIPA's mandates without a rational basis violated the Illinois Constitution's prohibition on special legislation. Defendants also argued that BIPA was unconstitutionally vague because the exclusion related to information collected under the Health Information Portability and Accountability Act (HIPAA) could reasonably be interpreted to apply not only to patient data but also to biometric information collected from pharmacist-employees.

The Circuit Court of Cook County previously held that both interpretations were reasonable but ruled that the legislature intended the HIPAA exemption to apply only to patient information. A decision on the constitutional issues remains pending.

Insurance coverage for BIPA disputes

In *Zurich American Insurance Company, et al., v. Omnicell Inc.*, the insurance company sought declaratory relief that it did not owe a duty to defend or indemnify Omnicell, Inc. in an underlying BIPA suit. The court granted a motion to stay pending resolution of the underlying case, *Mayza v. Northwestern Lake Forest Hospital, et al.*

What this means to you

The number of class action cases filed since the *Rosenbach* decision continue to mount against companies, including employers who utilize biometric scanners for identity verification purposes. Compliance with the statute is necessary to avoid significant damages and litigation costs. We recommend that entities that collect biometric information take the following actions:

Determine whether an exemption from BIPA's mandates applies.

Determine whether biometric information from employees, contractors or others is collected, stored or shared.

Determine the time frame over which liability could be imposed if notice and disclosure requirement have not been implemented for mitigation purposes.

Develop a written policy available to the employees, contractors and the public regarding retention and destruction schedules for permanently destroying biometric information.

Prior to collection of biometric information, disclose the intent and purpose for the collection of the biometric information, and obtain a written release consenting to the collection, use and storage of the information and acknowledging receipt of the retention and destruction schedules.

Contact us

If you have questions about your obligations under BIPA or would prefer assistance in adopting policies and practices to comply with the law or to mitigate liability, contact Michael Hayes, Bob Tomaso, Anne Mayette or your Husch Blackwell attorney.

Tracey Oakes O'Brien is a contributing author of this content.