DALEY MOHAN GROBLE
IN IT WITH YOU.

DMG BIOMETRIC LAW UPDATE

Illinois Supreme Court Decision Brings a Wave of Biometric Privacy Class Actions

By: Laura Platt

Technology has become ubiquitous in the workplace including as an integral part of business security systems. Because of technological progress, companies increasingly use biometric information for multiple purposes. Biometrics are biological markers that make each of us unique and distinguishable from one another, the most common being the finger print. Their uniqueness makes them ideal for identification systems, but they are also easily copied and used for improper purposes, such as in identity theft. Worse, once breached and distributed, they cannot be replaced or changed, like a social security number can, as they are exclusively ours for our entire life.

It is now common for security systems to rely, in part, on biometric technology to authenticate authorized users, or employees, before granting them access to company facilities, computer systems and protected business information. At least in Illinois, because of legislation, the use of biometric technology has exposed companies to substantial liability risks, and the situation intensified recently as a result of the Illinois Supreme Court's decision in *Rosenbach v. Six Flags Entertainment Corp.,* 2019 IL 123186. In *Rosenbach*, the court severely restricted previously successful defenses to biometric privacy claims, and the opinion has led to a wave of class action lawsuits against companies in all sorts of businesses and industries.

BIPA Basics

If you have ever found yourself asking Apple's Siri for driving directions, using your fingerprint to unlock your smart phone, or adding a Snapchat filter to your photo, then you have interfaced with biometric technology. Biometric technology captures, records, and stores the private physiological information of its users, such as finger and voice prints, and facial patterns.

(Continued)

The increased use of biometric data in the workplace and in business, and the need to protect such data from disclosure, caught the attention of legislators in Illinois.

In 2008, the Illinois General Assembly passed the Biometric Information Privacy Act ("BIPA"). The statute is codified at 740 ILCS 14/1 *et seq*. BIPA prohibits private entities from collecting and storing "biometric identifiers" without prior notification and written consent. BIPA defines "biometric identifiers" as a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. The Act's provisions apply to any biometric information regardless of how it is captured, converted, stored or shared.

As a precondition of obtaining the biometric information, any private entity collecting the information must: (1) make their data retention policy publicly available; (2) notify individuals in writing what biometric information is being collected, how the information is being stored and for how long, the use of such information, and how the information will be destroyed; (3) refrain from selling biometric information to third parties; and (4) handle the biometric information with reasonable care. The Act provides that the biometric data must be destroyed when the initial purpose for collecting or obtaining such information has been satisfied, or within three years of the individual's last interaction with the private entity, whichever occurs first.

BIPA provides for a private cause of action against any private entity that violates any of its provisions. The Act provides for liquidated damages of $1,000 or actual damages (whichever is greater) per "negligent" violation of the Act, and the greater of $5,000 or actual damages per "intentional" or "reckless" violation of the Act. Courts have yet to determine whether the liquidated damages will be awarded on a per person violation or on a per person per day violation basis. In addition, a prevailing plaintiff is entitled to reasonable attorney's fees and costs, including expert witness fees.

Illinois remains the only state in the nation that allows for a private cause of action for violation of a biometric privacy law. Since 2017, over 200 BIPA violation cases have been filed in Cook County alone. Most of those cases were filed as class actions, and most sought purely liquidated damages. The extent of this private right of action is a matter of dispute, the resolution of which required cases to make their way up through the appellate process. One of the arguments defendants have successfully raised is that a plaintiff must suffer actual damage in order to bring a claim for a statutory violation. In a key turning point, however, the Illinois Supreme Court has now rejected that defense.

Rosenbach v. Six Flags

In *Rosenbach*, the Supreme Court resolved conflicting decisions of the First and Second appellate districts, and held that "an individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an 'aggrieved' person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act." In other words, the biometric data need not have been stolen, hacked or otherwise misappropriated or misused for there to be a valid cause of action under BIPA. All that is needed is an alleged violation of the provisions of BIPA.

The Court unanimously found that to impose the burden of an actual injury beyond the violation of the Act would be both inconsistent with the statutory language and contrary to clear legislative intent, and would frustrate the purpose of the Act.

Since the January 25, 2019 decision in *Rosenbach*, more than 50 additional lawsuits have been filed in Cook County for violation of BIPA, nearly all of them as class actions on behalf of persons whose biometric information was collected by their employer. The cases allege failure to obtain consent for collecting biometric information, insufficient disclosure of retention and destruction policies and/or failure to destroy the biometric information once an employee has left the employer.

In the face of the uptick of BIPA lawsuits, companies would be wise to review their current biometric data policies, including the written consent they obtain prior to collection, and their written disclosure and information destruction policies. Companies should include in this review a consideration of third-party vendors who have access to this information and whether they are in compliance with the provisions of BIPA.

Federal Court Disposes of Two BIPA Claims Pursuant to Railway Labor Act

By: Matthew J. Hammer

Two recent decisions from the Northern District of Illinois offer a glimpse into how courts could limit employee class actions under the Illinois Biometric Information Privacy Act ("BIPA"). In those cases, the courts dismissed claims against airlines on the ground they were subject to mandatory arbitration under the federal Railway Labor Act ("RLA"). The recent decisions suggest that collective bargaining agreements ("CBAs") may provide fertile defensive grounds against employee statutory actions, even for industries where the collective bargaining process is not governed by the RLA.

Congress passed the RLA to promote stability in labor-management relations by providing a comprehensive framework for resolving labor disputes involving airlines and railroads. The RLA framework includes "major" and "minor" disputes. Major disputes are those that create contractual rights, such as rates of pay, rules or working conditions. Major disputes, ultimately, may be considered by the courts. Minor disputes, on the other hand, grow out of the interpretation or application of existing CBAs and when resolution of a claim requires interpretation of a CBA, the claim is subject to mandatory and exclusive arbitration under the RLA. Embedded in the RLA is a strong preference for arbitration, as opposed to judicial resolution of disputes. In *Johnson v. United Air Lines*, a union baggage

handler at O'Hare International Airport filed a BIPA lawsuit seeking statutory damages on behalf of himself and those similarly situated arising out of United's timekeeping practices. United, like many employers, utilized plaintiff's fingerprints to track when he signed in and out of work. In collecting the fingerprint data of its employees, United allegedly did not obtain employee consent before using and transmitting the biometric information, as required by BIPA. United moved to dismiss the claim pursuant to the RLA, arguing that the BIPA claim was a "minor dispute" under the plaintiff's CBA.

The court agreed. Citing rather boilerplate language in the CBA, the court ruled that "there is no way for the Plaintiff to pursue a BIPA claim without interpreting the existing CBA between United and [plaintiff's union]." Indeed, the applicable CBA provided United with the "sole and exclusive right to manage, operate, and maintain the efficiency of the business and working forces," including the ability to "maintain discipline and efficiency in the Company's facilities." In exercising these rights, United opted for a timekeeping system utilizing fingerprint technology. Thus, any challenge to the use of fingerprints as a means of managing the efficiency of its business and work forces would require interpretation of the CBA in arbitration proceedings as mandated by the RLA.

In a puzzling subsequent order, the court remanded the case to the Circuit Court of Cook County, Illinois because the baggage handler did not allege a "concrete injury" but sought only statutory damages. The court's conclusion appears to be at odds with the Illinois Supreme Court's decision in *Rosenbach v. Six Flags*, in which it held that a plaintiff suffers a "real and significant" injury when "a private entity fails to adhere to the statutory procedures" in BIPA. This may be the federal court's message to the Illinois court that, if no actual damages exist, the state court can handle the cases, but should not preclude the preemption defense in the state court.

In *Miller v. Southwest Airlines*, ramp and operations agents represented by a labor union filed a BIPA lawsuit based on Southwest's biometric timekeeping and payroll system that required employees to scan their fingerprints to sign in and out of work. The employees also filed common law claims for intrusion upon seclusion, conversion, negligence, fraud, and breach of contract. In the face of allegations similar to those in *Johnson*, Southwest moved to dismiss, arguing that the claims were subject to mandatory arbitration under the relevant CBAs and the RLA. Notably, and contrary to the *Johnson* order, the court determined that the employees alleged a concrete injury, such that the court had jurisdiction over the claims.

Relying on case law including *Johnson* and broad, commonplace CBA language, the court determined that the employees' claims constituted minor disputes preempted by the RLA because they required interpretation of and reference to the CBAs that governed the employees' rates of pay, rules, and working conditions.

(Continued)

To resolve the claims, the court would have to:

- interpret the scope of the union's authority as the "sole and exclusive bargaining agent" to consent to the use of the timekeeping system on behalf of the employees;
- determine whether Southwest acted within its authority under the CBAs, including within its broad grants of authority to "manage and direct the work force" and to govern covered employees "by all reasonable Company rules and regulations";
- consider the parties' bargaining history with respect to wages and working conditions;
- interpret the CBAs' wage provisions; and
- interpret the CBAs' grievance system and arbitration procedure.

Accordingly, the court dismissed the BIPA and common law claims and ordered that the claims be submitted to arbitration. The court also denied the employees leave to file a second amended complaint asserting only a BIPA claim, reiterating that the claim remains preempted by the RLA.

The plaintiffs in *Miller v. Southwest* appealed the district court's decision and the case is currently pending before the Seventh Circuit Court of Appeals.

Significantly, BIPA preemption may not be limited to cases governed by the RLA. Implicit in the *Miller* and *Johnson* rulings is the principle that unions may bargain away their members' statutory rights under BIPA. This is in accord with other Illinois decisions. *E.g., Matthews v. Chicago Transit Authority*, 2016 IL 117638 (2016), ¶68 (recognizing that "a union can waive statutory and economic rights on behalf of its members"). Whether unions can waive their members' BIPA rights is one of the issues that is likely to be addressed by the Seventh Circuit in *Miller*.

These decisions concerning the RLA and BIPA are encouraging for railroads, airlines, and other industries where labor issues are governed by CBAs, but this is obviously a developing area of Illinois privacy law. DMG continues to follow developments in this area, including the Seventh Circuit's consideration of the *Miller v. Southwest Airlines* decision, the *Johnson v. United Air Lines* litigation, and the BIPA litigation environment forming in the wake of *Rosenbach v. Six Flags*.

Is That BIPA Lawsuit Subject to Insurance Coverage or Indemnification?

By: Robert J. Prendergast

The rise in class action lawsuits under the Illinois Biometric Privacy Act (BIPA), and the potential for increased exposure after the Illinois Supreme Court's decision in *Rosenbach v. Six Flags Entertainment Corp.*, 2019 IL 123186, means companies should look aggressively at their risk management programs to find potential insurance or indemnity coverage for those claims. Coverage may exist under general liability, cyber or employment practices policies, and indemnity rights may arise under contracts with vendors providing payroll, security or data management services. BIPA class actions are a developing breed, though, so companies looking to shift those losses to an insurer or contract party may be hard-pressed to fit them within existing policy and contract language.

Two pending lawsuits present a good example of this sub-category of BIPA litigation. In *Krause v. Caputo's New Farm Produce, Inc.*, the plaintiff asserts a class action against Caputo's (employer) and ADP (provider of biometric timeclock services) for violation of BIPA. In *Westfield Insurance Company v. Caputo's New Farm Produce, Inc.*, Westfield (Caputo's CGL insurer) seeks a declaratory judgment that the BIPA lawsuit is not covered under the "personal and advertising injury" provisions of Caputo's policy, and that Westfield has no duty to defend Caputo's. Personal and advertising provisions typically provide coverage for "an oral or written publication of material that violates a person's right of privacy."

The BIPA plaintiffs alleged that Caputo's failed to properly inform its employees of the purpose and duration of storing the biometric data, and improperly disclosed the data to a third-party vendor (ADP). Westfield alleged in the declaratory judgment case that coverage was barred under the following exclusions, thereby precluding any obligation to defend:

- Knowing violation of the right of another
- Material published prior to the policy period
- Recording and distribution of material or information in violation of law
- Employment-related practices, policies, acts or omissions
- Access or disclosure of confidential or personal information

These actions are both in the very early stages, and thus far there have been no cross-claims for indemnity between Caputo's and ADP, but the cases illustrate the many challenges to obtaining coverage for BIPA claims.

(Continued)

As with CGL policies, potential for coverage under cyber liability policies can vary based on the nature of the allegations and be impacted by many of the same exclusions as a CGL policy. A cyber liability policy may cover unauthorized access, or inadvertent disclosure, but may not provide coverage where the allegations concern obtaining and storing information without consent. And under *Rosenbach*, BIPA liability does not require improper disclosure or misuse of the biometric data.

Employment practices policies also vary, and some could provide coverage for employment related misrepresentation or violations of employment privacy. Violations of state and federal law could be an exclusion, however, which might preclude coverage for BIPA claims.

BIPA exposure is a growing concern and requires a focused and strategic company response. Even though companies may struggle to secure insurance or indemnity coverage under existing policies and agreements, they should structure their practices going forward to ensure that any future claims are properly covered. That includes working with risk management and insurance professionals to determine what coverage is available and economically viable.

It also means drafting the company's contracts with vendors involved in their use of biometric data to make sure the vendor:

- Takes responsibility for securing compliance with all statutory requirements
- Agrees to indemnify the company for any failure to comply
- Names the company as additional insured under policies covering BIPA claims

Please contact Daley Mohan Groble with any questions about the above topics or other issues of interest at info@daleymohan.com or visit our website www.daleymohan.com