BLANKROME

Biometric Privacy

OCTOBER 1, 2020 • NO. 3

Latest Challenge Shows Staying Power of CBA Preemption Defense in Biometric Class Actions

Relying on a successful preemption defense, Jackson Park SLF, LLC ("Jackson Park") recently defeated a biometric privacy suit claiming it improperly used employees' fingerprints to track time and attendance without first providing notice, receiving consent, or publishing its retention schedules in violation of the Illinois Biometric Information Privacy Act ("BIPA").

The opinion—Williams v. Jackson Park SLF, LLC, *2020 WL 5702294 (N.D. Ill. Sept. 24, 2020)*—*is the latest in a string of successful preemption challenges and demonstrates the staying power of this defense to procure outright dismissals where BIPA litigation is brought by unionized employees.*

OVERVIEW OF FINGERPRINT DATA

Biometric fingerprint technology involves using "biometrics" (*i.e.,* individual physical characteristics) to scan a person's finger and identify their finger "geometry" by measuring its length, width, thickness, and surface area. These measurements are then converted into a mathematical algorithm referred to as a "digital template" and stored in a database.

To identify or verify a fingerprint, an algorithm compares the new template created from extracted data points with a previously stored digital template.

PREEMPTION AS A BASIS TO DISMISS BIPA CLAIMS

Christopher Williams, a former Jackson Park employee, sued on behalf of himself and other similarly situated Jackson Park employees for alleged BIPA violations arising from Jackson Park's use of its biometric fingerprint time and attendance system.

Jackson Park moved to dismiss Williams' complaint, arguing his BIPA claim was preempted by Section 301 of the Labor Management Relations Act ("LMRA"). Section 301 preempts state law claims—requiring them to be resolved before an adjustment board, not a court—if resolution of the claim requires the interpretation of a collective bargaining agreement ("CBA").

The court agreed, finding Williams' claim analogous to the Seventh Circuit's decision in *Miller v. Southwest Airlines Co.,* 926 F.3d 898 (7th Cir. 2019). In *Miller,* union members used their fingerprints to clock in and out of work. The *Miller* plaintiffs alleged Southwest "implemented these [timekeeping] systems without their consent, failed to

publish protocols, and use third-party vendors to implement the systems"—mirroring the claims brought by Williams. In finding preemption, the Seventh Circuit held "how workers clock in and out is a proper subject of negotiation between unions and employers," thus requiring the dispute to go before an adjustment board for resolution.

The *Williams* court also rejected plaintiff's argument his claim should not be preempted because the union cannot waive his privacy rights under BIPA. In doing so, the court again pointed to *Miller,* which addressed this argument directly when it held BIPA's text allowed authorized agents, such as unions, to act on members' privacy rights.

The court also rejected Williams' anti-preemption argument that because Jackson Park's CBA did not anticipate the use of biometric information, the defense was inapplicable, noting the *Miller* court had also addressed this question when it determined that whether a CBA management rights clause gave consent regarding biometric data is itself a question for an adjustment board.

The court next rejected Williams' argument that if his claim was preempted, he would not have a viable form in which to seek relief—as the CBA's seven-day window to raise claims could completely bar him from pursuing administrative remedies. Here, the court noted the initial forum for Williams to bring his claim was specified in the CBA grievance procedures. Because there was no evidence Williams followed those procedures, he could not pursue his claims in court. Further, even if the grievance procedures were not available, the court had no authority to confer subject matter jurisdiction on itself to entertain Williams' case. This was especially so considering the Seventh Circuit had already rejected this type of "remedial gap" argument in *Healy v. Metro. Piet & Exposition Auth.,* 804 F.3d 836 (7th Cir. 2015).

Finally, the court rejected Williams' attempt to avoid preemption by pointing to the fact that he was not a union member for the first month of his employment, when his biometrics were being collected, stored, used, and disseminated allegedly in violation of BIPA. The court found this argument unpersuasive because Williams did not dispute he was a union member for a majority of his employment and he sought to represent a class of all employees working in Illinois—whether they were union members or not. Consequently, Williams' BIPA complaint was dismissed for lack of subject matter jurisdiction.

TAKEAWAYS

Williams is the latest in a string of favorable decisions dismissing BIPA suits by unionized employees on preemption grounds following the Seventh Circuit's decision in *Miller.* In just 2020 alone, at least four other BIPA actions have been kicked out of court based on successful preemption challenges.

Williams continues the trend of favorable treatment of the preemption defense in BIPA litigation involving employees working under CBAs; it also illustrates the power of preemption challenges to defeat litigation by unionized workers for violations of Illinois' biometric privacy statute.

Ultimately—as demonstrated by *Williams*—the preemption defense can be an effective tool for defending mere technical/procedural BIPA violations in situations requiring interpretation of a CBA.

ACTION STEP: ENSURING THE ABILITY TO RAISE A PREEMPTION CHALLENGE TO BIPA CLAIMS BROUGHT BY UNIONIZED WORKERS

To successfully challenge BIPA suits based on preemption, unionized employers should ensure the proper steps are taken during the collective bargaining process to preserve the ability to assert the defense in the event the employer's biometrics practices are tested in court. As an initial matter, employers should give unequivocal, advance notice to union representatives of any intent to incorporate the use of biometric data into their operations. Employers should also thoroughly address issues of BIPA notice and consent during collective bargaining negotiations—especially with respect to the union's consent, on behalf of the represented employees, for the employer to collect and use the workers' biometric data for business purposes.

Issues of notice and consent should also be addressed in the employer's written CBA with the union. Employers should ensure clear, unequivocal language is included in the CBA establishing that the union has consented to the company's use of its employees' biometric data for business purposes.

Approached properly, unionized companies that leverage the benefits of biometrics to add value to their business operations can provide themselves with a powerful defense against BIPA class actions.

HOW WE CAN HELP

As leaders in the biometric privacy space, Blank Rome's dedicated Biometric Privacy Team has developed a comprehensive understanding of the core strategies relied on by plaintiffs' attorneys to litigate biometric class actions, as well as the applicable defenses to defeat and/or limit a range of different biometric class claims. Our biometric privacy litigators utilize this in-depth knowledge of the most significant and complex issues that arise in all types of biometric litigation to develop winning litigation strategies, aggressively defend clients, and posture cases for dispositive dismissals or favorable settlements.

At the same time, our Biometric Privacy Team can also provide key counseling and guidance regarding the collection, use, and storage of all types of biometric data, as well as today's new wave of biometric privacy laws. We can also assist in developing tailored, comprehensive biometric privacy compliance programs that ensure continued, ongoing compliance not just with current biometrics regulations, but anticipated laws as well—allowing you to stay ahead of this constantly-evolving legal landscape.

For more information on BIPA, assistance in defending BIPA class action litigation, or enhancing and updating your biometric privacy compliance program, or to discuss any other biometric privacy issues in more detail, please contact a member of Blank Rome's Biometric Privacy Team.

For additional information, please contact:

Jeffrey N. Rosenthal, Philadelphia Office
Partner and Team Lead, Biometric Privacy
215.569.5553 | rosenthal-j@blankrome.com

David J. Oberly, Cincinnati Office
Associate, Biometric Privacy
513.362.8711 | doberly@blankrome.com