Quarterly Review

Volume 15 Issue No. 3 Autumn 2020

Ohio Association *of* Civil Trial Attorneys

A Quarterly Review of Emerging Trends in Ohio Case Law and Legislative Activity...

Contents

OACTA
Ohio Association of Civil Trial Attorneys
The Source for Defense Success

Strategies for Defending Illinois Biometric Privacy Class Action Lawsuits

David J. Oberly, Esq.
Blank Rome LLP

Over the last two years, companies utilizing biometric data in their operations have faced a relentless wave of class action lawsuits for purported violations of the Illinois Biometric Information Privacy Act ("BIPA"). 2019 was an especially rough year for BIPA defendants, as courts issued a string of plaintiff-favorable decisions that greatly expanded the scope of potential BIPA liability, while limiting many of the major defenses.

As just one example, after several significant setbacks, Facebook agreed to pay $650 *million* to settle a longstanding BIPA dispute over the use of facial recognition technology to support its photo "tagging" feature.

However, 2020 has been a different story for defendants in BIPA class actions, who have seen a sizable shift in momentum with courts issuing a number of favorable decisions on key issues and defenses. Several recent BIPA opinions demonstrate how some of these defenses—namely preemption, arbitration, and personal jurisdiction—can be utilized by corporate defendants to halt such claims in their tracks or, at a minimum, significantly limit the amount of damages involved in this type of litigation.

Why Ohio Businesses Should Take Note of Recent BIPA Developments

While the name of the law suggest that BIPA applies only to companies located in Illinois, the reach of the law extends well beyond the borders of the Prairie State. Specifically, any Ohio business that collects or uses the biometric data of residents of Illinois must comply with the mandates of BIPA. As such, those Ohio companies that fall under the scope of BIPA should take note of the defenses that have recently emerged as powerful methods to successfully defend or limit BIPA lawsuits and work with experienced biometric privacy counsel to leverage these powerful defenses whenever possible.

Overview of the Illinois Biometric Information Privacy Act

Under BIPA, private entities cannot collect, possess, use, share, or store biometric data without first implementing a publicly-available privacy policy, providing notice, obtaining a written release, making certain disclosures, and maintaining reasonable security measures.

BIPA has quickly become the next class action battleground—primarily due to the statute's private right of action permitting the recovery of statutory damages ranging between $1,000 and $5,000 by any "aggrieved" person under the law. These uncapped statutory damages, combined with a low bar for establishing harm, led to an explosion of bet-the-company BIPA class litigation in 2019, which continued apace into 2020—until very recently.

Leveraging the Preemption Defense to Dispose of BIPA Class Litigation

One of the strongest defenses that has emerged on the scene in BIPA litigation is preemption.

The BIPA preemption defense finds its roots in the Seventh Circuit Court of Appeals' opinion in *Miller*

CONTINUED

v. Southwest Airlines Co., 926 F.3d 898, 901 (7th Cir. 2019). In that case, the Seventh Circuit directly addressed the preemptive impact of federal labor law, and the Railway Labor Act ("RLA") in particular, on claims asserted by union employees subject to a collective bargaining agreement (CBA) alleging state-law violations of BIPA. In *Miller*, union employees of United Airlines and Southwest Airlines brought suit against their airline employers alleging violations of BIPA stemming from their use of biometric timekeeping systems.

On appeal, the Seventh Circuit held that the union workers' BIPA claims were completely preempted by the RLA. In doing so, the court first noted that BIPA allowed worker or *their authorized agent* to receive necessary notices and consent to the collection and use of biometric data under the statute. Applied to the airline workers' claims, whether the unions *did* consent to such collection and use of their biometric data, or perhaps granted authority through a management-rights clause, was a question that was required to be answered by an adjustment board under the RLA.

The court reasoned that because the plaintiffs had asserted a right in common with all other employees, dealing with a mandatory subject of collective bargaining, it was not possible, even in principle, to litigate a dispute about how the airlines acquired and used fingerprint data for its whole workforce without asking whether the union had consented on its employees' collective behalf. As such, the BIPA claims were preempted by federal labor law, and were required to be resolved by an adjustment board, and not before a judge pursuant to the RLA.

Following *Miller*, several decisions have been issued in 2020 dismissing BIPA lawsuits in their entirety due to preemption under the RLA, including *Crooms v. Southwest Airlines Co.*, 2020 WL 2404878 (N.D. Ill. May 12, 2020), and *Frisby v. Sky Chefs, Inc.*, 2020 WL 4437805 (N.D. Ill. Aug. 3, 2020).

Importantly, courts have also followed *Miller* in extending the scope of the preemption defense to claims implicating § 301 of the Labor Management Relations Act ("LMRA")—which preempts claims founded directly on rights created by CBAs, as well as those that are substantially dependent upon an analysis of a CBA.

In *Peatry v. Bimbo Bakeries USA, Inc.*, 2020 WL 919202 (N.D. Ill. Feb. 26, 2020), a former employee of Bimbo Bakeries, USA filed suit for purported violations of BIPA stemming from the bakery's biometric timekeeping practices. Peatry worked for the company from September 2016 to February 2019, and was covered by a CBA from May 2018 through her employment end date. The bakery moved to dismiss Peatry's lawsuit, arguing that the LMRA preempted Peatry's claims.

The *Peatry* court agreed, holding that LMRA § 301 preempted the plaintiff's claims during the period over which Peatry was working under a CBA. The court found that *Miller* governed the court's resolution of the preemption question because the RLA preemption standard is "virtually identical to the preemption standard the Court employs in cases involving § 301 of the LMRA." Consequently, under *Miller*, Peatry's claims required interpretation of the CBA governing the bakery workers' employment, such that § 301 preempted Peatry's claims during the period the CBA was in effect.

Following *Peatry*, several other BIPA actions have been dismissed based on successful LMRA preemption challenges, including *Gray v. Univ. of Chicago Medical Center, Inc.*, 2020 WL 1445608 (N.D. Ill. March 25, 2020), and *Williams v. Jackson Park SLF, LLC,* 2020 WL 5702294 (N.D. Ill. Sept. 24, 2020).

Utilizing Arbitration Agreements & Class Action Waivers to Kick BIPA Lawsuits Out of Court

Second, defendants have also found success in utilizing arbitration agreements and class action waivers to kick BIPA class action lawsuits out of court and into binding individual arbitration.

CONTINUED

Such was the case in *Miracle-Pond v. Shutterfly, Inc.*, 2020 WL 2513099 (N.D. Ill. May 15, 2020), where a federal court held a plaintiff was required to pursue her BIPA claims in individual arbitration, despite the fact the arbitration provision was not added to the company's Terms of Use until a year *after* the plaintiff originally agreed to them.

In *Shutterfly*, Vernita Miracle-Pond sued Shutterfly claiming the company's use of its facial recognition technology in connection with the Shutterfly account she maintained violated BIPA. To complete her account registration process, Miracle-Pond had to agree to Shutterfly's Terms of Use, which included both a revision clause and a class action waiver. Significantly, the revision clause stated Shutterfly "may revise these Terms from time to time by posting a revised version" and explained a user's continued use of the app subsequent to any such revisions constituted the user's acceptance of the changes. The revision clause did not require notice of revisions to Shutterfly users beyond posting the new terms.

The 2014 Terms did not, however, include an arbitration provision; this provision was added to Shutterfly's Terms of Use in 2015 and was thereafter included in every later version of the Terms.

After the filing, Shutterfly moved to compel arbitration and stay the federal litigation pending the outcome. In so doing, Shutterfly argued that, as a user of the app, Miracle-Pond had agreed to Shutterfly's Terms of Use—including the provision mandating individual arbitration. The District Court agreed with Shutterfly, granting its motion to compel arbitration for Miracle-Pond and staying the federal court proceedings.

In its opinion, the court first found that Shutterfly's Terms of Use constituted a valid and enforceable clickwrap agreement. The court highlighted that Shutterfly's page presented the Terms of Use for viewing, stated that clicking "Accept" would be considered acceptance of the Terms of Use, and offered both "Accept" and "Decline" buttons. Thus, Miracle-Pond agreed to be bound by Shutterfly's Terms of Use when she created her account.

The court also found that it was proper to require Miracle-Pond to arbitrate her claim, even where the 2014 Terms of Use did not include an explicit arbitration provision. Pursuant to the change-in-terms provision in the 2014 Terms of Use, Miracle-Pond agreed her continued use of Shutterfly's services would communicate her assent to the most recent version of the Terms posed online at the time of her use. Because Miracle-Pond continued to use her account after Shutterfly posted its amended Terms in 2015, she accepted those modifications, including the inclusion of the 2015 arbitration clause.

Lastly, the court held that it was also proper to require Miracle-Pont to to arbitrate her claim, even where Shutterfly failed to provide notice of the 2015 modification and she was never informed of the change. Here—because the parties' agreement expressly reserved the right of Shutterfly to modify its terms—Miracle-Pond was bound to the 2015 modifications, as Shutterfly had posted the modified terms on its website in 2015 and Miracle-Pond indicated her acceptance thereof by continuing to use Shutterfly's services.

As such, the court held Miracle-Pond had entered into a valid arbitration agreement, thus compelling the court to grant Shutterfly's motion to compel arbitration.

Personal Jurisdiction as a Basis to Dismiss BIPA Claims

Lastly, defendants have also found success in challenging personal jurisdiction to extricate themselves from BIPA class action lawsuits at an early junction in the litigation.

Such was the case in *McGoveran v. Amazon Web Services, Inc.*, 2020 WL 5602819 (S.D. Ill. Sept. 18, 2020), where Amazon Web Services ("AWS") and Pindrop Security, Inc. ("Pindrop") defeated a biometric privacy lawsuit claiming they captured voice data through phone calls placed through AWS' Amazon Connect service in violation of BIPA.

CONTINUED

Pindrop offers voiceprint biometric services for call centers to confirm the identity of callers. AWS provided cloud storage services under the brand Amazon Connect for Pindrop to store its collected voiceprint data.

In *McGoveran*, three plaintiffs sued AWS and Pindrop for alleged BIPA violations stemming from the collection and retention of their voiceprint data from multiple calls made to a John Hancock call center located in Massachusetts, which used Amazon Connect with Pindrop biometric voiceprint authentication.

After the filing, AWS and Pindrop moved to dismiss for lack of personal jurisdiction. The Southern District of Illinois agreed with AWS and Pindrop, granting their respective motions and dismissing both defendants.

In its opinion, the court focused its attention to whether plaintiffs had made a *prima facie* showing of personal jurisdiction over AWS/Pindrop sufficient to avoid dismissal. Because the plaintiffs conceded general jurisdiction was lacking, the court focused its analysis on whether the defendants were subject to specific personal jurisdiction in Southern District of Illinois.

On this issue, the court rejected the plaintiffs' principal argument that defendants were subject to specific jurisdiction because they collected/possessed the voiceprint data of Illinois citizens who placed phone calls while in the state. The court reasoned the plaintiffs' initial dialing of the phone while in Illinois—the only activity at issue that took place in the Prairie State—was insufficient by itself to confer specific jurisdiction.

In addition, the court also found neither the defendants' relationship with a third party located out of state (John Hancock) nor that third party's contacts with Illinois could be used to establish personal jurisdiction.

Thus, in the absence of any evidence AWS or Pindrop specifically targeted Illinois citizens when providing their voice printing services, and because the litigation did not arise from contacts AWS or Pindrop themselves created with Illinois, the court concluded it lacked personal jurisdiction over both defendants, resulting in dismissal of the entire action.

Takeaways

Following Facebook's $650 million BIPA settlement, companies that collect and use biometric data can expect to continue to see a flurry of BIPA class action lawsuits to continue for the foreseeable future. With that said, while the Facebook settlement will further incentivize plaintiff's attorneys to pursue BIPA lawsuits for mere technical violations of the law, as the above decisions show, several potential avenues exist to attack and defeat, or at least limit, a broad assortment of BIPA actions. As such, BIPA defendants and their legal counsel are well advised to add the above defenses to their litigation toolbelts and should contact experienced counsel about utilizing these potentially game-changing defenses whenever possible.

David J. Oberly, Esq., is an attorney in the Cincinnati office of Blank Rome LLP and is a member of the firm's Biometric Privacy, Privacy Class Action Defense, and Cybersecurity & Data Privacy groups. David's practice encompasses both defending clients in high-stakes, high-exposure biometric privacy, privacy, and data breach class action litigation, as well as counseling and advising clients on a wide range of biometric privacy, privacy, and data protection/cybersecurity matters. He can be reached at doberly@blankrome.com.