AN A.S. PRATT PUBLICATION
NOVEMBER-DECEMBER 2020
VOL. 6 • NO. 9

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 6 **NUMBER 9** **NOVEMBER - DECEMBER 2020**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [5] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [245] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2020–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Designing a BIPA Defense: Using Preemption and Arbitration to Defeat Biometric Class Actions

By Jeffrey N. Rosenthal and David J. Oberly [*]

Since the Illinois Supreme Court issued its seminal decision in *Rosenbach v. Six Flags Entertainment Corp.*[1] in the beginning of 2019, companies using fingerprint scanners and other biometric technologies have faced a relentless deluge of class actions for purported violations of the Illinois Biometric Information Privacy Act ("BIPA").

BIPA

BIPA has quickly become the next class action battleground – primarily due to the statute's private right of action, which permits the recovery of statutory damages between $1,000 and $5,000 per violation, along with attorney's fees. Since *Rosenbach*, most BIPA decisions have been extremely plaintiff-friendly, including the U.S. Court of Appeals for the Ninth Circuit's opinion in *Patel v. Facebook, Inc.*[2] – which, like *Rosenbach*, held that any BIPA violation is sufficient to constitute a sufficient injury-in-fact for Article III standing.

More recently, however, the tide may have started to turn in favor of defendants – with courts issuing favorable decisions in 2020 on several key BIPA issues and defenses.

One of those cases is *Crooms v. Southwest Airlines Co.*,[3] in which the court held four plaintiffs were required to pursue their BIPA claims against their employer before an adjustment board or in arbitration – not in federal court. This resulted in the dismissal of the entire action. *Crooms* serves to highlight the continued favorable treatment of preemption/arbitration defenses, and exemplifies how they can be deployed in BIPA actions.

---

* Jeffrey N. Rosenthal is a partner at Blank Rome LLP and leads the firm's Biometric Privacy Team. He concentrates his complex corporate litigation practice on consumer and privacy class action defense. David J. Oberly is an attorney at the firm advising sophisticated clients on a wide range of cybersecurity, data privacy, and biometric privacy matters. The authors may be reached at rosenthal-j@blankrome.com and doberly@blankrome.com, respectively.

[1] 129 N.E.3d 1197 (Ill. 2019).

[2] 932 F.3d 1264 (9th Cir. 2019), *cert. denied*, No. 19-706 (U.S. Jan. 21, 2020).

[3] N.D. Ill. May 12, 2020.

Preemption and Arbitration as a Basis to Dismiss BIPA Claims

In *Crooms*, four employees of Southwest Airlines alleged their employer violated BIPA by requiring their fingerprints be scanned by a biometric timekeeping device without first obtaining their consent or making a written biometrics privacy policy available. Three employees started their careers with Southwest as ramp agents before being promoted to ramp supervisor; the fourth started as a ramp supervisor. Critically, Southwest ramp agents are represented by a union and covered by a collective bargaining agreement ("CBA"), while ramp supervisors are not.

Southwest moved to dismiss, arguing first that the Railway Labor Act ("RLA") – which imposes mandatory arbitration for disputes concerning rates of pay, rules, or working conditions – preempted the BIPA claims of the three employees represented by the union when they worked as ramp agents, thus requiring them to seek relief before an adjustment board – and not in federal court.

Southwest relied heavily on the U.S. Court of Appeals for the Seventh Circuit's decision in *Miller v. Southwest Airlines Co.*,[4] where the court held an adjustment board – not a federal court – was required to decide whether Southwest's union had consented to the use and collection of employee biometric data. The *Miller* court reasoned the question of consent necessarily involved an interpretation of the CBA, and a dispute about the interpretation or administration of a CBA must be resolved by an adjustment board under the RLA, as there is "no room for individual employees to sue under state law" under such circumstances.

Crooms agreed with Southwest, finding the CBA covered the working conditions of the three plaintiffs who started their careers as ramp agents, just like the plaintiffs in *Miller*. As such, the existence and scope of consent as it pertained to those three plaintiffs were questions for an adjustment board based on the RLA.

Southwest also moved for dismissal based on arbitration agreements all four employees accepted when they became ramp supervisors. Southwest maintains an alternative dispute resolution ("ADR") program for all non-union employees, which requires employees to arbitrate certain covered claims. Each of the plaintiffs electronically signed an acknowledgement form by checking a box, agreeing to comply with the ADR program.

Crooms also agreed with Southwest on its arbitration argument, holding that the arbitration agreements at issue covered the plaintiffs' BIPA claims. In doing so, the court first concluded the two employees who had agreed to the ADR program after Southwest updated its program in 2018 to expressly apply to claims under BIPA had clearly agreed to arbitrate any BIPA disputes.

[4] 926 F.3d 898 (7th Cir. 2019).

The other two employees, however, had agreed to the airline's ADR program before the 2018 program went into effect. And the old version of Southwest's ADR program did not expressly mention BIPA and did not explicitly refer to claims about biometric data. As such, these two employees argued the old ADR program did not cover their BIPA claims. The court found this argument unpersuasive, as the question of whether the old ADR program covered BIPA claims amounted to a dispute about arbitrability – or, in other words, whether they agreed to arbitrate the dispute.

Importantly, the terms of the old ADR program had language providing that the parties also agreed to arbitrate the question of arbitrability. Thus, it was up to an arbitrator – not the court – to decide whether the two employees agreed to arbitrate their claims under BIPA when they agreed to the pre-2018 ADR program.

As such, the fourth employee (who not required to arbitrate his claims before an adjustment board) was nevertheless required to arbitrate his claims before an arbitrator. In addition, the court also noted that were not for the RLA, the other three employees would have been required to arbitrate their claims before an arbitrator as well.

TAKEAWAYS

Crooms follows on the footsteps of *Miller v. Southwest Airlines Co.*, *Peatry v. Bimbo Bakeries, Inc.*,[5] and *Gray v. Univ. of Chicago Medical Center, Inc.*[6] – all of which also dismissed BIPA class lawsuits based on successful preemption challenges.

As discussed, *Miller* directly addressed the preemptive impact of the RLA on BIPA claims asserted by union employees subject to a CBA, and held the union workers' BIPA claims were completely preempted by the RLA where questions existed as to whether their union consented to the collection and use of their biometric data – which were required to be resolved by an adjustment board.

In *Peatry* and *Gray*, the U.S. District Court for the Northern District of Illinois extended the preemption defense to claims implicating Section 301 of the Labor Relations Management Act ("LRMA"). The *Crooms* decision continues this trend of favorable treatment of the preemption defense in BIPA litigation involving unionized employees under CBAs, and further demonstrates defendants' ability to defeat such suits by unionized employees via this robust defense.

Crooms also offers valuable insight into the scope of the arbitration defense that can be applied in BIPA litigation to defeat claims involving unionized and non-unionized workforces. Significantly, *Crooms* illustrates that BIPA defendants can dispose of class

[5] No. 1:19-cv-02942 (N.D. Ill. Feb. 26, 2020).
[6] No. 1:19-cv-04229 (N.D. Ill. March 25, 2020).

actions at an early stage by demonstrating resolution of workers' BIPA claims must be handled through arbitration where the workers have executed arbitration agreements covering biometric privacy disputes.

Lastly, from a compliance perspective, companies using biometrics in the course of their operations can apply the *Crooms* court's analysis as a template for minimizing the scope of liability posed by Illinois' biometric privacy statute.

First, *Crooms* illustrates the importance of addressing BIPA in corporate policies and describing the company's ability to collect and use employees' biometric data during the collective bargaining negotiation process. Employers should also ensure all collective bargaining agreements include express language specifying that the union has consented to the collection and use of biometric data on behalf of those employees represented by the union.

Second, *Crooms* demonstrates that all employers – even those with non-union workforces – should require workers to sign employment agreements containing arbitration provisions with class action waivers as a condition of employment in order to limit BIPA risk.