AN A.S. PRATT PUBLICATION
MAY 2022
VOL. 8 NO. 4

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 8 **NUMBER 4** **May 2022**

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*, [8] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [113] (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

(2022–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, 631.291.5541. 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.

Employers Take Heed: Follow Illinois Biometric Privacy Rules or Risk a Losing Battle

By Adam S. Forman, Nathaniel M. Glasser and Matthew Savage Aibel*

Since its enactment in 2008, the Illinois Biometric Information Privacy Act has given rise to a lot of litigation, including many employment class action suits. The authors of this article discuss one such class action that was the subject of an important decision issued recently by the Illinois Supreme Court, and what it means for employers.

Employers in Illinois who collect, use, or retain their employees' biometric data – personal information such as fingerprints or facial or voice recognition – need to be aware of a recent legal development.

Illinois was the first state to enact a law restricting the collection and storage of biometrics, and it remains the frontline for advancement of jurisprudence on the subject. The Illinois Biometric Information Privacy Act ("BIPA")[1] requires entities, including employers, that collect biometric data to follow a number of protocols, including maintaining a written policy about the collection and storage of biometric data, providing owners of biometric information (in this case employees) with written notice of such practices, and obtaining informed consent from individuals subject to biometric data collection. Since its enactment in 2008, BIPA has given rise to a lot of litigation, including many employment class action suits.

THE ILLINOIS SUPREME COURT'S INTERPRETATION OF BIPA FAVORS PLAINTIFFS

One such class action was the subject of an important decision issued recently by the Illinois Supreme Court. In *McDonald v. Symphony Bronzeville Park LLC*,[2] the state's

---

* Adam S. Forman (aforman@ebglaw.com) is a member of the firm at Epstein Becker Green representing employers in employment litigation and traditional labor matters and advising clients on emerging technologies and their impact in the workplace. Nathaniel M. Glasser (nglasser@ebglaw.com), a member of the firm and co-leader of its COVID-19 Compliance and AI practice groups, handles workforce compliance counseling, employment-related litigation, internal investigations, and employment-related due diligence. Matthew Savage Aibel (maibel@ebglaw.com) is an associate at the firm representing clients in commercial litigation, business disputes, and breach-of-contract matters, and also in matters involving discrimination, harassment, retaliation, whistleblowing, and wage and hour disputes.

[1] https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

[2] 2022 IL 126511, https://ilcourtsaudio.blob.core.windows.net/antilles-resources/resources/0f7c99c2-f9a1-423f-88e8-f52e108737ac/McDonald%20v.%20Symphony%20Bronzeville%20Park,%20LLC,%202022%20IL%20126511.pdf.

highest court issued a unanimous opinion that effectively eliminated an entire defense in BIPA lawsuits. The lawsuit was a putative class action brought by an employee against her health care facility employer. As part of its security and timekeeping systems, the employer scanned employee fingerprints. In an amended complaint, the employee alleged that she was never provided the opportunity to give informed, written consent to the storage of her biometric data. This amendment is significant because the original complaint included allegations of mental anguish, as noted in a brief concurring opinion penned by Justice Michael J. Burke. Those alleged workplace injuries would have precluded the employee from her action under BIPA, pursuant to the Illinois Workers' Compensation Act's ("IWCA")[3] exclusive remedy provision. Whether IWCA's exclusive remedy provision provided the employer with a defense by precluding the employee from seeking only statutory damages under BIPA was the question before the Illinois Supreme Court. The court said no, yet it remains an open question if the IWCA would bar claims for damages that were non-statutory, i.e., those for emotional distress.

WHAT DOES THIS MEAN FOR EMPLOYERS?

McDonald is further evidence of the court's position that BIPA should be liberally construed, as was made clear in a prior case, *Rosenbach v. Six Flags Entertainment Corp.*[4] In that case, the Illinois Supreme Court also unanimously held that plaintiffs do not need to suffer an actual injury beyond a violation of rights provided for by BIPA in order to state a claim under that statute. With *Rosenbach*, the Illinois Supreme Court established its position that a technical violation of BIPA creates a "real and significant injury" in and of itself.

BIPA is one of only a few laws nationwide that afford a private right of action to the owners of biometric data. This in itself constitutes a risk for businesses that use biometric technology for any purpose. Lawsuits can come from aggrieved individuals as well in the form of collective classes that allege violations of BIPA, even if those purported violations caused no actual harm to the plaintiffs, and even if the plaintiffs are not just employees, but customers, visitors, or anyone else from whom any biometric data is collected. The Illinois Supreme Court has been consistent in construing BIPA liberally, and the *McDonald* decision, which provides a roadmap for plaintiffs seeking statutory damages, further cements BIPA as a potential minefield for employers that fail to heed its requirements.

---

[3] https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2430&ChapterID=68.

[4] 2019 IL 123186, https://www.illinoiscourts.gov/Resources/f71510f1-fb2a-43d8-ba14-292c8009dfd9/123186.pdf.

The best litigation strategy is to avoid litigation in the first place through compliance. Violations of BIPA can be very costly, with statutory damages of at least $1,000 per violation ($5,000 if the violations are deemed intentional or reckless), plus attorneys' fees and costs. BIPA is an attractive vehicle for the Illinois plaintiffs' bar and, as such, a substantial risk for businesses.

THE RISK IS NOT LIMITED TO ILLINOIS BUSINESSES

While it is obvious that BIPA presents a significant challenge to employers doing business in Illinois, it is important to note that biometric privacy laws have been enacted elsewhere, including Texas, Washington State, and New York City. Other states or localities are likely to follow suit, and developments in Illinois set the trend. Thus, what applies to employers in the Land of Lincoln today may well be widely applicable within the next few years.

WHAT ILLINOIS EMPLOYERS (AND OTHERS) SHOULD DO RIGHT NOW

- *Assess*: Review all company practices surrounding the collection, usage, storage, or transmission of any biometric information covered by BIPA or other state and local laws like it. This might be as seemingly benign as issuing employees devices, such as smartphones with built-in thumbprint or facial recognition technology, or providing time clocks or security measures with those features.

- *Write*: Be sure that your company has clear written policies that address the procedures for collection, storage, use, transmission, and destruction of biometric data, including specific timeframes.

- *Communicate*: Be sure to notify all individuals – employee or otherwise – about your biometric data policy, including information about how such data will be secured to protect individual privacy interests.

- *Obtain Consent*: BIPA and certain other laws require that individuals whose biometric data may be collected, stored, or used in any way provide informed consent to such collection, storage, and usage. Be sure to inform those individuals and to get their consent in a format that can be stored and, if necessary, produced as evidence of compliance with BIPA in the event of litigation.

- *Consult*: Consult with counsel to assist with risk assessment, policy development, and training to ensure compliance with this important law.