AN A.S. PRATT PUBLICATION
SEPTEMBER 2023
VOL. 9 NO. 7

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 9 **NUMBER 7** **September 2023**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Alexandra Jefferies at ..... (937) 560-3067
Email: ..... alexandra.jefferies@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
LexisNexis® Support Center ..... https://supportcenter.lexisnexis.com/app/home/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3385

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*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [82] (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

(2023–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.

Claim Under Illinois Biometric Information Privacy Act Accrues With Each Scan or Transmission of Private Information, Illinois Supreme Court Rules

By David C. Layden, Caroline L. Meneau and Annie Kastanek*

In this article, the authors discuss the decision by the Illinois Supreme Court holding that a separate claim accrues under the Illinois Biometric Information Privacy Act each time a private entity scans or disseminates an individual's biometric identifier or information in violation of Sections 15(b) or (d) of the law.

In *Cothron v. White Castle System, Inc.*,[1] the Illinois Supreme Court resolved the question of when claims for violations of Sections 15(b) and (d) of the Illinois Biometric Information Privacy Act (BIPA) accrue.

In a 4-3 decision, the court held that a separate claim accrues each time a private entity scans or disseminates an individual's biometric identifier or information in violation of Sections 15(b) or (d).

BACKGROUND ON BIPA AND THE *COTHRON* LITIGATION

The Illinois legislature enacted BIPA in 2008 to regulate the collection, retention, and use of biometric data. BIPA has proved to be very popular with plaintiffs' class action lawyers, and BIPA claims have resulted in numerous high-profile, high-value class settlements and a recent $228 million jury verdict.

In *Cothron*, the plaintiff filed a putative class action complaint on behalf of all Illinois employees of White Castle in the Circuit Court of Cook County. Challenging White Castle's use of a system that required employees to scan their fingerprints to access their pay stubs and restaurant computers, the complaint alleged violations of BIPA Sections 15(b) and (d). The case was removed to federal court.

White Castle moved for judgment on the pleadings, arguing that the plaintiff's claims were untimely because they accrued in 2008, when the plaintiff first used the technology and White Castle allegedly first obtained the plaintiff's biometric data and allegedly disseminated it to third-party technology vendors and storage providers. The plaintiff responded by arguing that the "continuing violation" rule applied, and therefore her

* The authors, attorneys with Jenner & Block LLP, may be contacted at dlayden@jenner.com, cmeneau@jenner.com and akastanek@jenner.com, respectively.

[1] Cothron v. White Castle System, Inc., 2023 IL 128004 (Feb. 17, 2023).

claims did not accrue until the last time that White Castle allegedly collected and disseminated her data without first complying with Sections 15(b) and (d). The plaintiff also argued, in the alternative, that every scan and every dissemination of that scan to third-party vendors constituted a separate violation of BIPA, and therefore at least a portion of her claims was timely.

The district court denied White Castle's motion, holding that the continuing violation rule did not apply, but finding that an entity violates Sections 15(b) and (d) each time it collects and disseminates biometric data without complying with the statute. The district court subsequently certified the issue for immediate interlocutory appeal.

On appeal, the U.S. Court of Appeals for the Seventh Circuit found that the parties' competing interpretations of BIPA were both reasonable and presented a novel and controlling issue of state law. It certified the claim-accrual question for resolution by the Illinois Supreme Court, and the Illinois Supreme Court chose to answer the question.

THE ILLINOIS SUPREME COURT'S *COTHRON* OPINION

In the *Cothron* decision, the Illinois Supreme Court held that, under the plain language of the statute, a party violates Sections 15(b) or 15(d) when it collects, captures, or transmits a person's biometric information without prior informed consent, and "each and every capture and use of plaintiff's fingerprint or hand scan," and each and every subsequent "transmission" of that data to a third-party, constitutes a separate violation of the statute.

Section 15(b) states that "[n]o private entity may collect [or] capture . . . a person's or a customer's biometric identifier or biometric information, unless it first" provides a specified written notice and obtains a written release. Defining the word "collect" in Section 15(b) to include "receiv[ing], gather[ing], or exact[ing]," and defining "capture" as "to take, seize, or catch," the court found that all scans – both the first print stored in a database and all subsequent authentication scans – involve collection or capture.

The court rejected White Castle's interpretation of the phrase "unless it first" as referring only to the first collection of biometric information. That phrase, the court explained, modifies the entity's obligation to obtain consent, not the triggering action.

The court reached the same conclusion as to Section 15(d), which provides that "[n]o private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless" it obtains informed consent from the individual or her legal representative or has legal authorization.

Rejecting White Castle's position that disclosure is a one-time event and defining "disclose" as to "expose to view," the court held that this provision's plain language

applies to "every transmission to a third party." The court also rejected arguments by White Castle that Section 15(d) applies only when information is disclosed to a new third party, not every time information is provided to the same vendor or other third party.

The majority acknowledged that its reading could result in the plaintiff in *Cothron* bringing claims on behalf of as many as 9,500 current and former White Castle employees, with class-wide damages exceeding $17 billion, but noted that "the statutory language clearly supports plaintiff's position." While noting that the "potential for significant damages awards" under BIPA should not dictate the legal interpretation of the statute, the court's holding includes two significant caveats regarding damages.

First, "[i]t appears that the General Assembly chose to make damages discretionary rather than mandatory," and, according to the court, "there is no language in the Act suggesting legislative intent to authorize a damages award that would result in the financial destruction of a business."

Second, a trial court presiding over a BIPA class action, as a "creature of equity," has the discretion to fashion a damages award that fairly compensates class members and deters future violations without destroying a defendant's business.

Ultimately, though, the court noted that policy-based concerns over "potentially excessive damage awards under the Act are best addressed by the legislature," and suggested that the General Assembly "review these policy concerns and make clear its intent regarding the assessment of damages" under BIPA.

Three justices dissented. They reasoned that the majority's decision could not be reconciled with the plain language of the statute, the purposes behind BIPA, or existing case law, and that it would lead to consequences far beyond what the legislature could have intended. The dissent reasoned that the purpose of BIPA is to prevent an individual's loss of the right to maintain privacy of their biometric data, and that once a private entity obtains a particular type of biometric data from an individual, the "secrecy interest is lost," and the entity is not obtaining anything new by collecting it again. The dissent also reasoned that the Illinois General Assembly could not have intended to impose punitive, crippling liability on businesses when it enacted BIPA. To the contrary, the legislature "recognized the utility of biometric technology and wanted to facilitate its safe use." Indeed, the penalty for selling biometric information to a third party without knowledge of the purpose for which it would be used is only $5,000 – a figure inconsistent with an interpretation of BIPA that makes available drastically higher damages for businesses that collect biometric information for their own business purposes.

CONCLUSION

Along with the Illinois Supreme Court's decision in *Tims, et al. v. Black Horse Carriers, Inc.*, which held that BIPA claims are governed by a five-year, rather than one-year, limitations period, the decision in *Cothron* is another in a line of Illinois Supreme Court decisions that have interpreted BIPA broadly and in ways that favor plaintiffs. It is likely to have significant impacts: It will broaden the set of claims that are timely. It also is likely to encourage the filing of even more BIPA class action cases. And it certainly will lead to many new disputes in existing BIPA cases, as both plaintiffs and defendants seek to use *Cothron* to advance their positions.

The Illinois General Assembly also likely will revisit the annual question of whether BIPA should be amended, and there will be extensive advocacy efforts directed to whether and how the law should be revised to prevent the "harsh, unjust, absurd, or unwise" consequences that the *Cothron* majority recognized its holding could create.