

AN A.S. PRATT PUBLICATION  
NOVEMBER/DECEMBER 2021  
VOL. 7 NO. 9

PRATT'S  
**PRIVACY &  
CYBERSECURITY  
LAW**  
REPORT



LexisNexis

**EDITOR'S NOTE: PRIVACY RIGHTS**

Victoria Prussen Spears

**THE EVOLVING RIGHT TO PRIVACY:  
FROM RELIGIOUS PRACTICE TO INTERNATIONAL  
TECH BRANDING TOOL**

Jason J. Oliveri

**IMPORTANT FTC RULES FOR HEALTH APPS  
OUTSIDE OF HIPAA**

Marissa C. Serafino, Ashley Thomas, and  
Shannon Britton Hartsfield

**DIGITAL TRANSFORMATION: KEY TECHNOLOGY,  
CYBERSECURITY, AND PRIVACY RISKS**

Imran Ahmad and Shreya Gupta

**CISA ISSUES PRELIMINARY CROSS-SECTOR  
CYBERSECURITY GOALS AND OBJECTIVES FOR  
CRITICAL INFRASTRUCTURE CONTROL SYSTEMS**

Scott Daniel Johnson

**PRIVILEGE AND THE TRIPARTITE  
INSURER-INSURED-COUNSEL RELATIONSHIP**

Matthew C. Luzadder and  
Cameron R. Argetsinger

**SEVENTH CIRCUIT COURT OF APPEALS  
WEIGHS ASKING ILLINOIS SUPREME COURT TO  
RESOLVE CONSTRUCTION OF THE BIOMETRIC  
INFORMATION PRIVACY ACT**

Michael W. O'Donnell, Jeffrey Brian Margulies,  
Andrea Laurie D'Ambra, and Marie Bussey-  
Garza

**MAINTAINING EMPLOYEE MEDICAL  
INFORMATION AND COVID-19**

Catherine F. Burgett, Fred Gaona III, and  
Darren S. Skyles

# Pratt's Privacy & Cybersecurity Law Report

---

---

VOLUME 7

NUMBER 9

November/December 2021

---

**Editor's Note: Privacy Rights**

Victoria Prussen Spears

293

**The Evolving Right to Privacy: From Religious Practice to International  
Tech Branding Tool**

Jason J. Oliveri

296

**Important FTC Rules for Health Apps Outside of HIPAA**

Marissa C. Serafino, Ashley Thomas, and Shannon Britton Hartsfield

300

**Digital Transformation: Key Technology, Cybersecurity, and Privacy Risks**

Imran Ahmad and Shreya Gupta

310

**CISA Issues Preliminary Cross-Sector Cybersecurity Goals and Objectives  
for Critical Infrastructure Control Systems**

Scott Daniel Johnson

314

**Privilege and the Tripartite Insurer-Insured-Counsel Relationship**

Matthew C. Luzadder and Cameron R. Argetsinger

318

**Seventh Circuit Court of Appeals Weighs Asking Illinois Supreme Court to  
Resolve Construction of the Biometric Information Privacy Act**

Michael W. O'Donnell, Jeffrey Brian Margulies, Andrea Laurie D'Ambra, and  
Marie Bussey-Garza

322

**Maintaining Employee Medical Information and COVID-19**

Catherine F. Burgett, Fred Gaona III, and Darren S. Skyles

326

## 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*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [293] (LexisNexis A.S. Pratt)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license. A.S. Pratt is a trademark of Reed Elsevier Properties SA, used under license.

Copyright © 2021 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. All Rights Reserved.

No copyright is claimed by LexisNexis, Matthew Bender & Company, Inc., or Reed Elsevier Properties SA, in the text of statutes, regulations, and excerpts from court opinions quoted within this work. Permission to copy material may be licensed for a fee from the Copyright Clearance Center, 222 Rosewood Drive, Danvers, Mass. 01923, telephone (978) 750-8400.

*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](http://www.lexisnexis.com)

MATTHEW  BENDER

(2021-Pub. 4939)

# *Editor-in-Chief, Editor & Board of Editors*

---

## **EDITOR-IN-CHIEF**

**STEVEN A. MEYEROWITZ**

*President, Meyerowitz Communications Inc.*

## **EDITOR**

**VICTORIA PRUSSEN SPEARS**

*Senior Vice President, Meyerowitz Communications Inc.*

## **BOARD OF EDITORS**

**EMILIO W. CIVIDANES**

*Partner, Venable LLP*

**CHRISTOPHER G. CWALINA**

*Partner, Holland & Knight LLP*

**RICHARD D. HARRIS**

*Partner, Day Pitney LLP*

**JAY D. KENISBERG**

*Senior Counsel, Rivkin Radler LLP*

**DAVID C. LASHWAY**

*Partner, Baker & McKenzie LLP*

**CRAIG A. NEWMAN**

*Partner, Patterson Belknap Webb & Tyler LLP*

**ALAN CHARLES RAUL**

*Partner, Sidley Austin LLP*

**RANDI SINGER**

*Partner, Weil, Gotshal & Manges LLP*

**JOHN P. TOMASZEWSKI**

*Senior Counsel, Seyfarth Shaw LLP*

**TODD G. VARE**

*Partner, Barnes & Thornburg LLP*

**THOMAS F. ZYCH**

*Partner, Thompson Hine*

---

*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. Copyright 2021 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. 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.

# Seventh Circuit Court of Appeals Weighs Asking Illinois Supreme Court to Resolve Construction of the Biometric Information Privacy Act

*By Michael W. O'Donnell, Jeffrey Brian Margulies, Andrea Laurie D'Ambra, and Marie Bussey-Garza*

*The U.S. Court of Appeals for the Seventh Circuit is considering a case that has the potential to convert a violation of the Illinois Biometric Information Privacy Act into a business-shuttering offense – without any demonstration of actual injury to the plaintiff. The authors of this article discuss the case, which is an important one to watch.*

The U.S. Court of Appeals for the Seventh Circuit heard oral argument on September 14, 2021, in *Cothron v. White Castle System, Inc.*,<sup>1</sup> a case that has the potential to convert a violation of the Illinois Biometric Information Privacy Act<sup>2</sup> (“BIPA”) into a business-shuttering offense – without any demonstration of actual injury to the plaintiff. While the case raises substantial equitable and constitutional questions, which were addressed in the briefing submitted by White Castle and its *amici*, the oral argument focused largely on whether the Seventh Circuit should address the issue before it or, instead, certify the question to the Supreme Court of Illinois.

The latter proposition has many businesses feeling anxious because the last time the Illinois Supreme court considered a major question regarding BIPA's construction, it adopted a broad reading that opened the floodgates to class action litigation under the statute. For businesses with operations in Illinois that use biometric technology, this case is an important one to watch.

---

\* Michael W. O'Donnell (mike.odonnell@nortonrosefulbright.com) is the partner in charge of the San Antonio office of Norton Rose Fulbright US LLP leading the commercial litigation practice there. Jeffrey Brian Margulies (jeff.margulies@nortonrosefulbright.com) is the partner in charge of the firm's Los Angeles and San Francisco offices focusing on litigation, compliance, and regulatory issues. Andrea Laurie D'Ambra (andrea.dambra@nortonrosefulbright.com) is the firm's U.S. Head of Technology & U.S. Head of eDiscovery and Information Governance focusing her practice on data privacy, e-discovery, cross border discovery, and cybersecurity. Marie Bussey-Garza (marie.bussey-garza@nortonrosefulbright.com) is an associate at the firm representing clients in complex commercial litigation matters and defending class actions.

<sup>1</sup> No. 20-3202, [https://scholar.google.com/scholar\\_case?case=11011131669740525425&hl=en&as\\_sdt=6&as\\_vis=1&oi=scholarrr](https://scholar.google.com/scholar_case?case=11011131669740525425&hl=en&as_sdt=6&as_vis=1&oi=scholarrr).

<sup>2</sup> <https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57>.

## BACKGROUND

Under BIPA, which was enacted in 2008, businesses must comply with certain statutory requirements in connection with the collection, use, or disclosure of biometric identifiers or information (e.g., through finger scans or facial recognition technology). These statutory requirements include providing specific disclosures and obtaining a written release from any individual prior to collecting that person's biometric information.<sup>3</sup>

In addition, BIPA specifies requirements that must be satisfied in order for an entity to disclose a person's biometric information.<sup>4</sup> "Any person aggrieved by a violation of" BIPA may bring an action to recover \$1,000 or actual damages for a negligent violation, \$5,000 or actual damages for an intentional or reckless violation, reasonable attorneys' fees and costs, and injunctive relief.<sup>5</sup>

In the first decade after BIPA's enactment, the statute was not heavily litigated. Then, in 2019, in *Rosenbach v. Six Flags Entertainment Corp.*,<sup>6</sup> the Illinois Supreme Court considered what it means to be "aggrieved" under the statute and determined that a "violation [of the statute], in itself, is sufficient to support the individual's or customer's statutory cause of action."<sup>7</sup> Following this decision, courts were flooded with BIPA class actions driven by the lure of potentially massive liquidated damages based on a purely statutory violation, even without any actual harm.

## THE ISSUE

In *Cothron*, BIPA's construction is once again at issue. This time, the question is whether a BIPA violation accrues only once, upon the first non-compliant collection or disclosure of biometric information, or whether each subsequent collection or disclosure constitutes a separate violation under the statute. For example, if an employer fails to get a BIPA-compliant written release from an employee prior to the employee's first use of a finger-scan time clock system, does the violation accrue upon the employee's first finger-scan, or is there a separate violation each time the employee scans his or her finger to clock in or out of work?

The district court held that each biometric scan constitutes a discreet violation of the statute subject to its own liquidated damages. Under this holding, if an employer uses a finger-scan timeclock system, each individual scan could constitute a separate violation of the statute subject to liquidated damages of up to \$5,000. If this reading stands, the potential damages, particularly in a class action, could be astronomical, thereby

<sup>3</sup> See 740 ILCS § 14/15(b).

<sup>4</sup> See *id.* § 14/15(d).

<sup>5</sup> See *id.* § 14/20.

<sup>6</sup> 129 N.E.3d 1197 (Ill. 2019).

<sup>7</sup> *Rosenbach*, 129 N.E.3d at 1206.

rendering the statute purely punitive, contravening its remedial purpose, and raising significant due process concerns.

## THE ORAL ARGUMENT

Although counsel for White Castle previewed the merits of these arguments, the panel quickly focused on whether the Illinois Supreme Court should have an opportunity to address this issue of statutory interpretation. Judge Frank Easterbrook, in particular, signaled that such an approach may be warranted, noting that BIPA cases are generally removed under the Class Action Fairness Act, thereby preventing the issue from reaching the state's highest court. White Castle argued that certification was inappropriate because resolution of the issue would merely require the court to apply state law accrual principals, which it does regularly. Cothron's counsel, on the other hand, welcomed certification of the issue, if the court were disinclined to uphold the district court's ruling.

## OTHER CONSIDERATIONS

While the ruling in this action may have broad-reaching effects on litigation in this space, the Illinois General Assembly may take action that will moot its outcome. Earlier this year, Illinois lawmakers introduced HB 559,<sup>8</sup> a bill that would, among other things, narrow the definition of biometric information and identifiers, implement a 30-day notice-and-cure period, and make liquidated damages available only upon a showing of a willful violation.

A separate bill, HB 560,<sup>9</sup> would eliminate the private right of action entirely, in favor of enforcement by the Illinois Department of Labor or Attorney General.

Prior attempts to amend BIPA, however, have been unsuccessful,<sup>10</sup> and HB 559 and 560 have drawn significant opposition from a number of sources, including the Illinois ACLU and organized labor.

This time may be different, however. As the global COVID-19 pandemic has led to unprecedented adoption of remote work, learning, court appearances, and various other human interactions, the use of video technology has been widely adopted. Indeed, the Seventh Circuit conducted oral argument in *Cothron* virtually by remote video conferencing technology. With the increased use of such technologies, a new wave of opportunistic BIPA lawsuits has emerged, including cases that target universities that have adopted remote exam proctoring software. These actions allege that the software,

<sup>8</sup> <https://www.ilga.gov/legislation/BillStatus.asp?DocNum=559&GAID=16&DocTypeID=HB&SessionID=110&GA=102>.

<sup>9</sup> <https://www.ilga.gov/legislation/billstatus.asp?DocNum=560&GAID=16&GA=102&DocTypeID=HB&LegID=128637&SessionID=110>.

<sup>10</sup> See, e.g., SB 2134 (2019), <https://www.ilga.gov/legislation/BillStatus.asp?DocNum=2134&GAID=15&DocTypeID=SB&LegID=120309&SessionID=108&SpecSess=&Session=&GA=101>.



which enables remote test-taking without a proctor, gathers students' biometric information, such as facial recognition data, voice data, and gaze monitoring data, without complying with BIPA's statutory disclosure and written release requirements.

Perhaps faced with these current realities, the Illinois General Assembly will be prepared to move forward with the amendments that have previously failed.

Alternatively, the changed landscape and tidal wave of litigation following *Rosenbach* may encourage the Illinois Supreme Court to adopt a more narrow construction if tasked with deciding the issue in *Cothron*.