AN A.S. PRATT PUBLICATION
JUNE 2023
VOL. 9 NO. 5

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT



EDITOR'S NOTE: SO, WHAT'S NEW?
Victoria Prussen Spears

NEW LEGAL REQUIREMENTS FOR ONLINE MARKETPLACES: THE INFORM CONSUMERS ACT
Maneesha Mithal, Rebecca Weitzel and Christopher N. Olsen

CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT: SIGNIFICANT CHANGES TO INCIDENT REPORTING ARE ON THE HORIZON
Michael J. Waters and Caitlin Smith

VETERANS AFFAIRS CONTRACTORS HAVE BROAD NEW CYBERSECURITY OBLIGATIONS
Eric S. Crusius

TOP 10 WAYS TO PROTECT ATTORNEY-CLIENT COMMUNICATIONS AFTER SUPREME COURT PUNTS CASE
Wendy Hughes, Samantha J. Monsees, Jeffrey Shapiro and Jeremy F. Wood

BIPA BECOMES THE MONSTER EMPLOYERS FEARED
Tyler Bohman, Matthew C. Luzadder and Whitney M. Smith

A BIOMETRIC LAW'S "ABSURD," "ANNIHILATIVE LIABILITY" FOLLOWING THE ILLINOIS SUPREME COURT'S DECISIONS IN *TIMS* AND *COTHRON*
Amir R. Ghavi, Michael A. Kleinman, and Katelyn E. James

DOJ MULTINATIONAL OPERATION TO DISRUPT RANSOMWARE ORGANIZATION FOCUSES ON AIDING RANSOMWARE VICTIMS
John P. Carlin, Jeannie S. Rhee, Steven C. Herzog and David K. Kessler

CROSS-BORDER DATA TRANSFER MECHANISMS AND REQUIREMENTS IN CHINA
Jenny (Jia) Sheng, Chunbin Xu and Wenjun Cai

Pratt's Privacy & Cybersecurity Law Report

VOLUME 9 **NUMBER 5** **June 2023**

Editor's Note: So, What's New?
Victoria Prussen Spears 147

New Legal Requirements for Online Marketplaces: The INFORM Consumers Act
Maneesha Mithal, Rebecca Weitzel and Christopher N. Olsen 149

Cyber Incident Reporting for Critical Infrastructure Act: Significant Changes to Incident Reporting Are on the Horizon
Michael J. Waters and Caitlin Smith 153

Veterans Affairs Contractors Have Broad New Cybersecurity Obligations
Eric S. Crusius 158

Top 10 Ways to Protect Attorney-Client Communications After Supreme Court Punts Case
Wendy Hughes, Samantha J. Monsees, Jeffrey Shapiro and Jeremy F. Wood 163

BIPA Becomes the Monster Employers Feared
Tyler Bohman, Matthew C. Luzadder and Whitney M. Smith 167

A Biometric Law's "Absurd," "Annihilative Liability" Following the Illinois Supreme Court's Decisions in *Tims* and *Cothron*
Amir R. Ghavi, Michael A. Kleinman, and Katelyn E. James 170

DOJ Multinational Operation to Disrupt Ransomware Organization Focuses on Aiding Ransomware Victims
John P. Carlin, Jeannie S. Rhee, Steven C. Herzog and David K. Kessler 174

Cross-Border Data Transfer Mechanisms and Requirements in China
Jenny (Jia) Sheng, Chunbin Xu and Wenjun Cai 177

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
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*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [82] (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 © 2023 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

MATTHEW BENDER

(2023–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 2023 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.

A Biometric Law's "Absurd," "Annihilative Liability" Following the Illinois Supreme Court's Decisions in *Tims* and *Cothron*

By Amir R. Ghavi, Michael A. Kleinman, and Katelyn E. James*

In this article, the authors use a hypothetical violation of the Illinois Biometric Information Privacy Act to illustrate the potential monetary impact of two recent decisions by the Illinois Supreme Court. They also offer some compliance and governance recommendations for consideration in light of those decisions.

The Illinois Supreme Court recently issued long-awaited decisions that will have a major impact on current and future lawsuits alleging violations of the Illinois Biometric Information Privacy Act (BIPA).[1] Following those decisions, two things are now clear: (1) all claims arising under BIPA have a five-year statute of limitations, and (2) each instance of repeated collection and disclosure of biometric information or identifiers together, (biometrics)[2] can give rise to a separate violation of the Act and corresponding fines.

As a reminder, BIPA requires businesses that collect, capture, disclose or disseminate biometrics to take certain steps to safeguard and protect such information.[3] Violations give rise to a private cause of action (meaning individuals can sue, not just an attorney general) and can lead to damages of up to $5,000 per violation.

Taken together, *Tims* and *Cothron* significantly expand, by several orders of magnitude, the number of potential claims and the amount of potential damages under BIPA, threatening "annihilative liability," in the words of the *Cothron* dissent. Although as

---

* The authors, attorneys with Fried, Frank, Harris, Shriver & Jacobson LLP, may be contacted at amir.ghavi@friedfrank.com, michael.kleinman@friedfrank.com and katelyn.james@friedfrank.com, respectively.

1 See Cothron v. White Castle System, Inc., 2023 IL 128004 and Tims v. Black Horse Carriers, Inc., 2023 IL 127801.

2 "Biometric identifier" is defined as "a retina or iris scan, fingerprint, voiceprint, scan of hand or face geometry." "Biometric information" is defined as "any information, regardless of how it is captured, converted, stored or shared, based on an individual's biometric identifier used to identify an individual."

3 Section 15(a) requires businesses in possession of biometrics to develop and make available a written policy that sets forth a retention schedule and destruction procedures; Section 15(b) requires informed consent before a business may "collect, capture, purchase, receive through trade, or otherwise obtain" biometrics; Section 15(c) prohibits the sale, lease, trade or profit from a person or customer's biometrics; Section 15(d) requires notice and consent before a business may "disclose, redisclose, or otherwise disseminate" biometrics; and Section 15(e) requires a business to use a "reasonable standard of care within [its] industry" with respect to the storage, transmission and protection of biometrics. The precise meaning of each of Section 15's requirements and prohibitions has been, and will continue to be, subject to judicial interpretation.

of this publication there has been only one BIPA case that has reached a jury verdict, companies that collect biometrics from Illinois residents should prepare for a deluge of putative consumer and employment class action cases accompanied by dramatically increased settlement demands by plaintiffs' attorneys.

This article illustrates the potential monetary impact of *Tims* and *Cothron* using a hypothetical BIPA violation and offers some compliance and governance recommendations for consideration in light of the Illinois Supreme Court's decisions.

FIVE-YEAR STATUTE OF LIMITATIONS

In *Tims*, the court held that the statute of limitations for all BIPA claims is five years, rather than one year, for violations of Sections 15(c) and (d). While acknowledging that (as Black Horse contended) a one-year statute of limitations plausibly could have applied to Sections 15(c) and (d) claims, the court reasoned that BIPA's legislative intent – specifically, concerns about the supposedly unknown increased risk of harm associated with the collection of biometrics back in 2008 – tipped the balance in favor of the five-year statute.

MULTIPLE CLAIM ACCRUAL

In *Cothron*, the court held that a separate claim accrues each time an individual's biometric is scanned or disclosed in violation of BIPA, rather than accruing the first time the biometric is collected, captured or disclosed.

Moreover, the court's decision can be read to mean that failure to obtain consent for the collection (required by Section 15(b)) and transfer to a third party (required by Section 15(d)) can give rise to two violations. White Castle estimated that the damages awardable to its 9,000 current and former class of employees would be between $19 million and $95 million if the plaintiff could recover under both Sections 15(b) and (d), and under one violation per employee, damages could equal close to $9.5 million.

In response, the majority found that BIPA's language was clear and therefore must be given effect even though the consequences may be "harsh," "unjust" or "absurd." Aside from noting that damages were made discretionary rather than mandatory under BIPA, meaning that a court has equitable discretion to fashion an award that deters future violations without destroying a defendant's business, the court left any policy-based concerns about excessive damages to the Illinois legislature to decide. Businesses should not rely on such relief coming any time soon.

Over the last few years, there have been numerous bills introduced in the Illinois legislature that have attempted to curtail BIPA's reach. These proposals have focused on, among other things, providing a notice to cure period for violations of BIPA, limiting the damages available to actual damages suffered (rather than liquidated damages) and including an exemption to allow for the collection of biometrics for a security purpose.

Although all have stalled or failed thus far, Illinois legislators continue to frequently introduce new proposals to narrow the law.

Until and unless any such bills are passed, the potential impact of *Cothron* and *Tims* on BIPA damages is staggering. Consider *Rogers v. BNSF Railway Co.*,[4] where a jury awarded $228 million to a class of approximately 45,600 truck drivers (i.e., liquidated damages of $5,000 per driver) whose fingerprint scans were transmitted to a third-party vendor purportedly without their written consent over a five-year period. The jury determined that BNSF violated the law 45,600 times – i.e., one time per driver.[5]

For illustrative purposes, under *Cothron* and assuming that (i) each truck driver scanned into the railway yard once per work day (using the American daily average of 260 work days per year) over a five-year period, and (ii) a reference image of each driver's fingerprint was transmitted to BNSF's third-party vendor each time a fingerprint was scanned, counting each scan and disclosure to BNSF's vendor as a separate violation, potential damages would have increased from $228 million to more than $592 billion.

ACTION ITEMS

Searching for a silver lining, legal and compliance departments should use *Rogers*, *Cothron* and *Tims* to seek "business" buy-in for a review of, and investment in, their company's biometrics compliance program. In particular, companies that collect or use biometrics from Illinois residents should consider the following action items:

- *Update Notice and Consent Forms*. Reviewing and updating BIPA notices and consent forms to make clear that notice and consent applies to the first and future collections and disclosures of biometrics. The court in *Cothron* did not have an occasion to address whether fresh notice and consent is also required each time a biometric is collected or disclosed, or if notice and consent at initial collection and disclosure is sufficient. However, in an earlier decision in *Cothron*, the U.S. District Court of Illinois stated in dicta that White Castle could have satisfied BIPA by providing employees with a consent form that would have been sufficient to cover "all future scans" of their fingerprints. This remains an open issue, and Senate Bill 1506, recently introduced, seeks to clear up any ambiguity by proposing an amendment to BIPA specifying that notice and consent should only be required upon the first collection or capture. In addition, companies should consider providing renewed notice and getting additional consent when a new biometric vendor is onboarded.

---

[4] Rogers v. BNSF Railway Co., No. 19-cv-03083 (N.D. Ill.).

[5] Notably, following *Cothron*, BNSF filed a notice of supplemental authority with the court in support of its motion for a new trial, seeking reduction of the $5,000 per driver jury verdict on the basis that, under *Cothron*, such damages were discretionary, and not mandatory.

- *Preserve Records*. Preserving records of BIPA notices, retention and destruction policies and proof of consent for a period of time commensurate with the five-year statute of limitations.

- *Negotiate Vendor Contracts*. Carefully reviewing and negotiating contracts with biometric vendors to seek clear and favorable allocations of compliance responsibility and business-friendly indemnity terms in the event of a BIPA violation.

- *Assess Potential Exposure*. Assessing potential exposure from past collection and disclosure practices and the availability of claims-made and occurrence-based Employment Practices Liability and Cyber insurance policies, noting in particular exclusions for liquidated damages, wrongful employment practices and wrongful data collection.

- *Revisit Use of Biometrics*. Weighing the benefits of biometrics to the business, potentially applicable exemptions under BIPA and the resources available to ensure compliance with BIPA's retention, destruction and security requirements and considering the availability of alternative authentication and access measures that do not involve the collection and disclosure of biometrics.

- *Evaluate Compliance with Other Biometrics Laws*. Evaluating applicability of and compliance with biometrics privacy laws in international, federal, state and even local jurisdictions. While laws in jurisdictions such as Texas, Washington, New York City and Portland, Oregon[6] directly regulate collection and disclosure of biometrics, many comprehensive privacy laws, such as the EU and UK General Data Protection Regulation, the California Consumer Privacy Act and Virginia's Consumer Data Protection Act, also include provisions requiring heightened protections of such information.

[6] In 2021, Portland became the first jurisdiction in the United States to prohibit the use of facial recognition technology by private entities and city agencies (subject to certain exemptions) in places of public accommodation.