AN A.S. PRATT PUBLICATION
MAY 2021
VOL. 7 • NO. 4

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 7 **NUMBER 4** **MAY 2021**

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

(2021–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.

Biometric Privacy Developments

By Mark A. Olthoff*

This article discusses biometric privacy litigation developments, identifies issues on the horizon in biometric privacy, and concludes with a discussion about Illinois Biometric Information and Privacy Act compliance.

Biometric privacy litigation has exploded in the last several years, with the current hot spot focus in Illinois. Class actions under the Illinois Biometric Information and Privacy Act ("BIPA") have flooded the Illinois state and federal courts since a January 2019 Illinois Supreme Court decision.

THE ILLINOIS STATUTE

The Illinois legislature passed the state's BIPA in 2008 to address the enhanced risk of identity theft associated with the collection and processing of biometric data (fingerprints, voiceprints, facial identifiers, retinal scan data, etc.). When biological data such as this is compromised, the attacker obtains a permanent marker for the affected individual. The Illinois legislature designed BIPA to require publicly posting a general notice and obtaining consent from the particular person whose biometric information was collected.[1]

And, importantly, BIPA provides for a private right of action to a person aggrieved by a violation of the statute.[2] The costs of BIPA non-compliance are significant, with uncapped statutory damages of $1,000 for a negligent violation and $5,000 for each intentional or reckless violation.[3] BIPA also permits the recovery of attorney fees, making it an attractive claim for attorneys seeking compensation for their clients.

RECENT DEVELOPMENTS

Several developments have occurred in the past year regarding BIPA litigation, including federal courts addressing the parameters of subject matter jurisdiction over BIPA claims, the statute of limitations issues, insurance coverage decisions and the applicability of preemption as a defense. This article initially discusses these recent

* Mark A. Olthoff is a shareholder at Polsinelli PC handling litigation of class actions, consumer protection, privacy laws, banking and securities laws, and all manner of business disputes. He may be reached at molthoff@polsinelli.com.

[1] 740 ILCS 14/15(a), (b).

[2] *Id.* at 14/20.

[3] *Id.*

developments, then identifies issues on the horizon in biometric privacy and concludes with a discussion about BIPA compliance.

Comparatively, with little litigation following the statute's enactment, this changed dramatically in 2019 when the Illinois Supreme Court decided a watershed case holding a mere violation of BIPA was enough to confer standing upon a plaintiff. An individual need not allege an actual injury beyond the violation of her statutory rights to be an aggrieved person under the law. Since that time, BIPA class actions have exploded in the state of Illinois.

Below are recent developments in BIPA litigation:

- Federal courts within Illinois, and the U.S. Court of Appeals for the Seventh Circuit, continue to examine issues regarding subject matter jurisdiction. Because the statute creates an Illinois cause of action, federal court jurisdiction is usually obtained upon removal under either ordinary diversity or the Class Action Fairness Act ("CAFA"). In both instances, however, the courts must review and scrutinize their subject matter jurisdiction, in particular, whether plaintiffs in BIPA cases have standing under federal law.

  In a case decided late last year, *Fox v. Dakkota Integrated Sys., LLC*,[4] the court found standing existed where the plaintiff alleged the defendant employer not only violated Section 15(a)'s publication requirements but also violated that law's data retention and destruction provisions. The defendant was alleged to have failed to publish its retention policies and retain biometric identifiers beyond the time permitted by statute and illegally disclosed them to a third party. The Seventh Circuit held these allegations sufficiently stated a concrete and personalized injury sufficient to create Article III injury supporting federal subject matter jurisdiction. The court concluded that unlawful retention of biometric data inflicts a privacy injury that is concrete and particularized reversing the district court's order remanding the case to state court.

  In the most recent decision, *Thornley v. Clearview AI, Inc.*,[5] the Seventh Circuit held that the allegations did not rise to sufficient concrete harm where the class plaintiffs asserted nothing more than procedural violations. The case presented a bit of procedural maneuvering. The class plaintiffs

[4] 980 F.3d 1146 (7th Cir. 2020).
[5] 984 F.3d 1241 (7th Cir. 2021).

initially filed a putative class action in state court alleging violations of three BIPA sections. Shortly after the first removal, the class plaintiffs voluntarily dismissed the complaint without prejudice and refiled a new and narrower complaint in state court specifically asserting that their cause of action was based upon a bare procedural violation divorced from any concrete harm. The defendant removed the second case. The plaintiff once again moved for remand arguing that the allegations did not give rise to Article III injury. The Seventh Circuit agreed with the district court's remand order, recognizing it, as the master of the complaint, the class plaintiffs had the right to assert the cause of action they wanted to pursue.

- Statutes of limitations are also a significant issue under BIPA as the statute includes no specific limitations period. Defendants have been asserting the appropriate statute of limitation for BIPA claims as one or two years. Meanwhile, plaintiffs contend that the five-year catch-all statute of limitations applies. The Illinois Supreme Court has not decided the applicable statute of limitations for BIPA claims. However, there are two cases on appeal to the Illinois intermediate appellate courts, and they will likely provide guidance. An additional issue is: when does a BIPA violation accrue and does a BIPA violation accrue when an individual's biometric information is first collected or each time it collects or discloses the data in violation of the statute? The Seventh Circuit is currently considering this accrual issue under a certified question.

- Many defendants have submitted BIPA claims to their insurance carriers. Usually, coverage has been denied. However, in a March 2020 Illinois appellate court decision, the panel held that an insurer had a duty to defend BIPA claims under the general liability policy's personal injury coverage provision. That intermediate appellate court decision is currently on appeal to the Illinois Supreme Court which granted review on September 30, 2020.

- Another issue of significance is preemption. This is because employees assert most BIPA claims and questions arise whether there is a federal labor law preemption or worker's compensation preemption under state law. With federal preemption, the Seventh Circuit has held the Labor Relations Management Act ("LMRA") preempts BIPA claims where the LMRA applies to the workforce. On the latter issue, courts in Illinois have generally determined that the state's worker's compensation act does not preempt BIPA claims. However, this issue has been appealed to the Illinois Supreme Court in a case watched closely.

WHAT'S NEXT IN BIOMETRIC PRIVACY?

While most of the litigation involving BIPA claims has occurred within Illinois, many other states have also passed privacy legislation or are currently considering it. Washington and Texas have biometric privacy statutes, but their laws have no private rights of action. The New York and Maryland legislatures are considering a biometric statute akin to Illinois that would include a private right of action. Other state legislatures have taken or are taking action in amendments to existing privacy or data breach response legislation, including in Arizona, Arkansas, California, Colorado, Delaware, Iowa, Nebraska, and Washington, D.C. Notably, the Illinois legislature now is considering a bill with serveral provisions that could slow the river of litigation, including a cure period, a specific limitations period, and limitations on penalties. Further developments on these statutes will be significant.

While most BIPA litigation involves fingerprints, e.g., employees clocking in or clocking out, other biometric makers can be the subject of biometric privacy cases. Perhaps the most recognized extension of the BIPA statute occurred in a suit against an American technology conglomerate where the company recently agreed to pay $650 million to settle claims involving facial recognition technology that could be used to make tagging suggestions for uploaded photographs. The *Clearview AI* case mentioned above involves a defendant that scraped photographic information from social media websites. An American multinational technology company has also been sued for collecting voice prints using products it offers. BIPA litigation will likely continue to evolve as new technologies hit the market.

CAN BIOMETRIC CLAIMS BE AVOIDED?

Mostly, biometric privacy statutes control and direct the disclosures and consents needed to collect and use biometric data. As discussed above, the Illinois BIPA does not prohibit the collection and use of biometric information if there are appropriate disclosures and consents provided by the individuals who are subject to the data collection. The statute provides specific guidelines for observing its requirements but compliance with the Illinois BIPA should include:

- A publicly available record retention policy;
- Specific disclosures to persons whose biometric data is to be collected, used, or stored;
- Written consent by the person whose information is being collected;

- Securely stored biometric data; and
- Retention or destruction of data under the company's data retention policy.

While compliance may be less problematic for employers that can more easily make disclosures and obtain consents from their employees, compliance becomes potentially more dubious for consumer-facing retailers. Providing required disclosures and obtaining written consents from users, customers, and others whose information may be unknown can be more difficult. So, particularly in the non-employee context, companies should know the specific statutes in the states in which they are operating, where they are collecting and using biometric data, and where they may sell or trade such information. Companies may consider posting signs in storefronts and adding disclosures to products sold. Including consents in "terms of use" for websites may also be helpful. Compliance with the statutes will require conscious efforts to follow the laws' requirements.