AN A.S. PRATT PUBLICATION
FEBRUARY/MARCH 2021
VOL. 7 • NO. 2

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 7 **NUMBER 2** **February/March 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.

Designing a BIPA Defense: Strategies for Third-Party Technology Vendors to Challenge Biometric Class Actions

By Jeffrey N. Rosenthal and David J. Oberly*

For some time now, employers have been the main target of a relentless wave of class action lawsuits by employees alleging violations of the Illinois Biometric Information Privacy Act ("BIPA") in connection with the use fingerprint scans for timekeeping purposes. Recently, however, employees and the plaintiff's bar have added a new primary target for such suits: third-party biometric timekeeping technology vendors.

To date, vendors' ability to avoid or limit liability under BIPA has been mixed. But there are several defenses that – while still being developed and refined by the courts – may prove useful for vendors to extricate themselves from bet-the-company BIPA suits or, at a minimum, trim the scope of potential liability.

OVERVIEW OF THE ILLINOIS BIOMETRIC INFORMATION PRIVACY ACT

BIPA regulates the collection, possession, disclosure, and security of biometric information; it is the only biometric privacy law in the country to provide a private right of action. In the beginning of 2019, the Illinois Supreme Court opened the floodgates to BIPA class actions when it issued *Rosenbach v. Six Flags Entertainment Corp.*,[1] which held plaintiffs can pursue BIPA claims even in the absence of any actual injury or damages.

After *Rosenbach*, hundreds of BIPA suits were filed in state and federal courts, the majority alleging mere technical violations of the law. Importantly – even without any actual harm – these suits pose tremendous exposure for defendants, as plaintiffs are permitted to recover statutory damages of $1,000 to $5,000 for "each violation."

Fortunately, several defenses have recently emerged that can be utilized by vendors to attack BIPA claims and, in some instances, have such suits dismissed in their entirety.

---

* Jeffrey N. Rosenthal is a partner at Blank Rome LLP and leads the firm's Biometric Privacy Team. He concentrates his complex corporate litigation practice on consumer and privacy class action defense. David J. Oberly is an attorney at the firm advising clients on a wide range of cybersecurity, data privacy, and biometric privacy matters. The authors may be reached at rosenthal-j@blankrome.com and doberly@blankrome.com, respectively.

[1] 129 N.E.3d 1197 (Ill. 2019).

MOTION TO DISMISS FOR FAILURE TO STATE A CLAIM – BIPA SECTIONS 15(a) and 15(d)

One of the primary methods third-party vendors have successfully attacked BIPA suits is through though Federal Rule of Civil Procedure 12(b)(6) motions to dismiss for failure to state a claim. Here, vendors can attack Section 15(a) and Section 15(d) claims – which apply to entities "in possession of" biometric data – and which are particularly susceptible to such challenges where the causes of action merely parrot the statutory language of BIPA or rely solely on "information and belief" allegations.

For example, in *Heard v. Becton, Dickinson & Co.*,[2] the court held plaintiff's allegations pertaining to purported violations of Sections 15(a) and 15(d) failed to satisfy the requirements of Rule 12(b)(6), thus mandating their dismissal. The *Heard* court reasoned that the plaintiff failed to allege the vendor exercised *any* dominion or control over his biometric data. Rather, most of plaintiff's allegations concerning possession merely parroted the statutory language.

Accordingly, because plaintiff failed to plead factual content that would allow the court to draw the reasonable inference the vendor was "in possession" of his biometric data, it dismissed the Section 15(a) and 15(d) claims. The *Heard* court also held plaintiff failed to state an actionable claim under Section 15(d) because he relied solely on "information and belief" allegations the defendant allegedly disclosed his biometric data – thus mandating dismissal of the Section 15(d) claim for a second, independent reason.

Similarly, in *Namuwonge v. Kronos, Inc.*,[3] the court dismissed a Section 15(d) claim under Rule 12(b)(6) where plaintiff merely alleged on information and belief that the defendant disclosed her biometric data to third parties, which the court found was insufficient to plausibly suggest her biometric data was, in fact, disseminated.

Importantly, in *Namuwonge* the plaintiff further alleged she and other employees "have no idea whether any Defendant sells, discloses, re-discloses, or otherwise disseminates their biometric data," which the court characterized as a "definitive" statement that solidified the conclusion the complaint lacked sufficient factual allegations to plausibly suggest the vendor disclosed or distributed her data to any third party.

Finally, the same result was also seen in *Bernal v. ADP, LLC.*[4] In that case, plaintiff's complaint contained only two allegations of unlawful disclosure under Section 15(d), both of which consisted of a single statement the vendor's technology "allows for and resulted in" the dissemination of plaintiff's biometric data to third parties. The court

[2] N.D. Ill. Feb. 24, 2020.

[3] 418 F. Supp. 3d 279 (N.D. Ill. 2019).

[4] Ill. Cir. Ct. Aug. 23, 2019.

held these allegations fell short of enough factual pleading because they were void of any facts to support a Section 15(d) violation by *actually* disclosing plaintiff's data.

MOTION TO DISMISS FOR FAILURE TO STATE A CLAIM – BIPA SECTION 15(b)

Often vendors do not collect biometric data directly from employees; instead, they only receive the data once it has been collected by the employer with whom the vendor has a business relationship.

Unlike Sections 15(a), (c), (d), and (e) of BIPA – all of which apply to entities "in possession of" biometric data – Section 15(b) applies to entities that "collect, capture, purchase, receive through trade, or otherwise obtain" biometric data. Here, vendors can attack Section 15(b) claims where the complaint fails to articulate any factual allegations the vendor "actively" collected the biometric data.

In the *Heard* case discussed above, the defendant third-party vendor successfully raised this very argument – specifically, that the Section 15(b) claim should be dismissed because the complaint did not plead sufficient facts the vendor itself actively collected plaintiff's biometric data. Significantly, the *Heard* court held that for Section 15(b)'s requirements to apply, an entity must – at a minimum – take an active step to "collect, capture, purchase, receive through trade, or otherwise obtain" biometric data. The court then found the plaintiff did not provide sufficient allegations the vendor took any such step. Rather, allegations regarding the vendor's purported collection of data merely parroted the statutory language and did not provide any specific facts to ground the plaintiff's legal claims, which mandated dismissal of the Section 15(b) claim.

LACK OF PERSONAL JURISDICTION

Another strategy with which third-party vendors have found success procuring dismissals is based on a lack of personal jurisdiction.

In *Bray v. Lathem Time Co.*,[5] the court granted a Georgia-based timekeeping system vendor's motion to dismiss based on a lack of personal jurisdiction. At issue in *Bray* was whether Illinois had specific personal jurisdiction over the vendor, which requires the defendant's contacts with the forum state show it purposefully availed itself of the privilege of conducting business in the forum state or purposefully directed its activities at the state.

In *Bray*, the vendor was incorporated and headquartered outside Illinois; did not have any real estate, accounts, personal property, employees, or physical presence in Illinois; did not target Illinois or purposely direct sales into the state through advertising/marketing or the use of sales or service representatives; and did not sell a timekeeping

[5] N.D. Ill. Mar. 27, 2020.

device to plaintiff's employer in Illinois. Under these facts, the court held it lacked specific personal jurisdiction over the vendor defendant.

Importantly, the court also rejected plaintiff's argument the vendor's operation of a website that could be accessed in Illinois was sufficient to establish jurisdiction – reasoning that the company had no additional physical presence in Illinois and did not intentionally target Illinois customers, such as by maintaining a sales or marketing program in the state. As such, the court dismissed the action against the vendor in its entirety for lack of personal jurisdiction.

INSUFFICIENT ALLEGATIONS OF INTENTIONAL OR RECKLESS CONDUCT

Finally, vendors can also attack BIPA actions by focusing on a complaint's lack of allegations of intentional or reckless conduct – which should mandate the dismissal of claims for statutory damages in the higher amount of $5,000 for intentional or reckless conduct.

Not every BIPA violation gives rise to a cognizable claim; only intentional, reckless, or negligent ones do. To recover statutory damages at the $5,000 level, a plaintiff must adequately allege an intentional or reckless violation of the statute. BIPA does not define "intentionally" or "recklessly." To plead recklessness or intent, a plaintiff must plead the elements of negligence (i.e., duty, breach of duty, and proximate cause), and then also plead a heightened state of mind.

To date, several third-party vendors have successfully asserted that a plaintiff's prayer for statutory damages in the amount of $5,000 for intentional or reckless violations should be stricken or dismissed where they failed to put forth any factual allegations of reckless or intentional conduct by the vendor. For example, in *Namuwonge* (discussed above), the court held plaintiff's abstract statements regarding damages – which were not supported by any substantive details to suggest the vendor's purported violations of BIPA were reckless or intentional – were insufficient for the court to infer that the vendor acted recklessly or intentionally, thus warranting the dismissal of claim for damages based on intentional and reckless conduct.

Similarly, in *Rogers v. CSX Intermodal Terminals, Inc.*,[6] the court held that where the plaintiff merely alleged the defendant's BIPA violations were knowing and willful – without providing any factual support – the plaintiff's conclusory statement regarding the intent was insufficient to allow the court to infer the defendant acted intentionally or recklessly.

[6] 409 F. Supp. 3d 612 (N.D. Ill. 2019).

CONCLUSION

As biometric technology continues to advance rapidly in terms of applicability and sophistication, the use of vendors' biometric systems will become increasingly more commonplace as employers and others seek to leverage the benefits of using fingerprints, facial scans, and other types of biometric data in their business operations. While this increased use will provide a significant boost to vendors' bottom lines, it will also greatly increase the likelihood vendors will find themselves on the receiving end of a potentially devastating BIPA class action.

As such, biometrics vendors are well-advised to consider implementing a proactive BIPA compliance program if they have not already done so. And if a vendor finds itself named as a defendant in a BIPA class action, it should work closely with experienced biometric privacy and class action litigation defense counsel to evaluate the defenses discussed above and determine their potential applicability to defeat or, at a minimum, significantly limit liability exposure.

Utilized properly, these defenses can be successfully employed at an early juncture in the litigation process and under a variety of circumstances.