AN A.S. PRATT PUBLICATION
JANUARY 2018
VOL. 4 • NO. 1

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 4 | NUMBER 1 | JANUARY 2018

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*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [4] (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

(2018–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, 718.224.2258. 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.

Second Circuit Set to Address Key Issues Under Illinois Biometric Information Privacy Act

By P. Russell Perdew, Chethan G. Shetty, and Michael McGivney*

The U.S. Court of Appeals for the Second Circuit recently conducted oral argument in a case under Illinois Biometric Information Privacy Act that the district court had dismissed. The authors of this article discuss the Act, the oral argument, and potential defenses in BIPA litigation.

The U.S. Court of Appeals for the Second Circuit became the first U.S. Court of Appeals to wade into the rising tide of litigation under Illinois Biometric Information Privacy Act ("BIPA") when it conducted oral argument on October 26, 2017 in a BIPA case that the district court had dismissed.[1] The Second Circuit at oral argument seemed prepared to affirm the district court's conclusion that plaintiffs lacked Article III standing because they did not allege any concrete injury. Many are eagerly anticipating the court's decision as it will be the first significant guidance regarding at least some of the issues that can arise in BIPA cases, which plaintiffs have been filing at a rapidly accelerating pace in recent months.

BIPA REGULATES PRIVATE ENTITIES' COLLECTION, STORAGE, AND USE OF BIOMETRIC INFORMATION

The statute narrowly defines biometric identifiers as *only* one of the following: "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[2] The definition is a closed list—not a list of examples—and also specifically excludes things like writing samples, photographs, or biological samples.[3] "Biometric information" is defined as any information based on a biometric identifier and used to identify an individual.[4]

The statute prohibits a private entity from capturing, buying, or otherwise obtaining a person's biometric identifier/information unless it first does the following: (1) develops a publicly available written retention schedule governing how long the information will be kept; (2) gives the person written notice that the information is

* P. Russell Perdew (rperdew@lockelord.com) is a partner at Locke Lord LLP litigating complex commercial, class action, and tort cases in jurisdictions across the country. Chethan G. Shetty (cshetty@lockelord.com) is an associate at the firm specializing in representing financial services companies in consumer-related class action litigation in both state and federal courts. Michael McGivney (michael.mcgivney@lockelord.com) is an associate at the firm where he is a member of the consumer finance and business litigation groups.

[1] *See Santana v. Take-Two Interactive Software*, No. 17-303 (2nd Cir.).

[2] 740 ILCS 14/10.

[3] *Id.*

[4] *Id.*

being collected or stored and of the purpose of doing so and how long the information will be kept; and (3) obtains a written release from the person.[5] BIPA also prohibits private entities from selling biometric identifiers/information, restricts any other disclosure thereof, and requires reasonable care be taken in storing or transmitting biometric identifiers/information.

BIPA creates a private right of action for any "person aggrieved" by a statutory violation and authorizes recovery of the greater of either actual damages or "liquidated damages" of $1,000 for a negligent violation or $5,000 for an intentional or reckless violation.[6] Reasonable attorneys' fees and injunctive relief are also available.[7]

BIPA is not the only statute governing biometric information, but it is the most onerous. Other statutes in Texas and Washington do not authorize a private right of action (state officials must enforce), and do not require a written release.[8]

A WAVE OF BIPA LITIGATION HAS ALREADY BEGUN

BIPA's remedies, along with employers' increasingly frequent use of biometrics for employee tracking purposes, seem to have contributed to a recent wave of putative class actions filed in Illinois courts alleging BIPA violations. So far this year, over a dozen putative class actions have been filed against employers alleging BIPA violations in connection with fingerprint scans used for time-keeping purposes. No industry is immune; recent class actions name retailers, a fast-food franchise, a trucking company, a nursing home, an airline cargo handling company, an ambulance company, a food manufacturer, and a supermarket chain.

POTENTIAL DEFENSES IN BIPA LITIGATION

Several defenses have been tried in BIPA cases thus far, some of which the *Take Two* court may offer guidance on. First, defendants have argued that BIPA's "person aggrieved" qualifier limits its private right of action to people with actual damages. This has met with mixed results.[9] These same two courts also split on whether a BIPA violation was a concrete harm sufficient to support federal subject-matter jurisdiction under *Spokeo v. Robins.*[10]

---

[5] 740 ILCS 14/15(a), (b).

[6] 740 ILCS 14/20.

[7] *Id.*

[8] Tex. Bus. & Com. Code Ann. § 503.001; Wash. Rev. Code Ann. § 19.375, *et seq*.

[9] *Compare McCollough v. Smarte Carte, Inc.* (N.D. Ill. Aug. 1, 2016) (dismissing BIPA action for lack of actual damages) *with Monroy v. Shutterfly, Inc.* (N.D. Ill. Sept. 15, 2017) (rejecting argument).

[10] 136 S.Ct. 1540 (2016).

Defendants have also argued that allegations fall outside the narrow definition of biometric identifier, though with little success at the pleadings stage.[11] This argument may be more successful on summary judgment.

Finally, defendants have argued that BIPA does not apply extraterritorially and that applying it in that way would violate the Dormant Commerce Clause of the U.S. Constitution. But these defenses are highly fact specific and therefore likely would not be successful in a motion to dismiss.[12]

IN *TAKE-TWO*, THE SECOND CIRCUIT MAY ADDRESS *SPOKEO* AND WHO A "PERSON AGGRIEVED" IS

In *Take-Two*, defendants made a video game that scanned players' faces to create a personalized in-game avatar. Although plaintiffs knew their faces were being scanned, they did not receive the specific notice or provide the written release required by BIPA. But the district court dismissed their case with prejudice, finding they lacked Article III standing, and were not "aggrieved" under BIPA, because any violations caused no harm. In other words, plaintiffs lacked both constitutional and statutory standing.

At oral argument, the Second Circuit peppered plaintiffs' counsel with questions regarding what harm, if any, plaintiffs suffered when they knowingly consented to the face scans, particularly since there was no subsequent data breach or significant risk of a breach. These questions suggest the court may affirm the district court's finding that plaintiffs lacked Article III standing under *Spokeo*. A ruling along these lines would significantly bolster defendants' threshold challenges to BIPA cases in federal courts.

The argument did not touch on the "person aggrieved" issue other than the Second Circuit's suggestion that the district court should not have reached that issue once it found no subject-matter jurisdiction under *Spokeo*. Thus, a plausible outcome will be the Second Circuit affirming dismissal under *Spokeo* but vacating the district court's finding that plaintiffs were not "aggrieved" under BIPA.

UPDATE: On November 21, 2017, the Second Circuit (in a non-precedential summary order) affirmed the dismissal of this case, agreeing with the district court that: (1) none of the alleged violations created a material risk of harm; and, (2) as a result, there was no federal subject-matter jurisdiction under *Spokeo*. The Second Circuit vacated the district court's conclusion that plaintiffs lacked a cause of action

[11] *See Rivera v. Google, Inc.*, 238 F. Supp. 3d 1088, 1095, 1100 (N.D. Ill. 2017) (denying motion to dismiss arguing face scan derived from a photo is not biometric information, but suggesting that discovery could change the analysis); *In re Facebook Biometric Information Privacy Litg.* (N.D. Cal. May 5, 2016) (same); *Monroy, supra* (rejecting argument that facial recognition scan was not a biometric identifier); *Norberg v. Shutterfly, Inc.*, (N.D. Ill. Dec. 29, 2015) (finding a plausible claim under BIPA based on face geometry derived from photographs).

[12] *See Monroy*, *supra* (agreeing that BIPA does not apply extraterritorially but declining to dismiss case because of the required factual inquiry); *Rivera*, 238 F. Supp. 3d at 1100-1102 (same).

under BIPA because the lack of injury meant plaintiffs were not "aggrieved" under the statute, finding that the district court should not have reached that substantive issue given the lack of subject-matter jurisdiction. This holding will help defendants make *Spokeo* arguments in other BIPA cases pending in federal court, but *Spokeo* is not binding in state courts, so the decision's impact in state court cases is less clear. The Second Circuit's holding that plaintiffs suffered no injury could also help defendants argue that plaintiffs whose data has not been compromised are not "aggrieved" under the statute, but the case is not binding on that point.