AN A.S. PRATT PUBLICATION
SEPTEMBER 2022
VOL. 8 NO. 7

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 8 **NUMBER 7** **September 2022**

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)

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

(2022–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, 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.

Recent Developments in Biometric Privacy Laws and What Companies Need to Know to Protect Themselves

By Michael G. Babbitt and J. Mylan Traylor*

In this article, the authors describe the requirements of the Illinois Biometric Information Privacy Act and the potential liability for companies, some of the most noteworthy cases and settlements, the most common and effective defenses against these types of lawsuits, and how companies can protect themselves against potential liability.

Several recent developments surrounding the Illinois Biometric Information Privacy Act ("BIPA"), and similar laws across the country, present new potential risks for companies of all types and sizes. Because of the recent uptick in BIPA lawsuits (both from employees and consumers), potentially large settlement amounts, and the limited types of defenses available to corporations, it is prudent for companies to stay informed as the law continues to develop in this area.

This article describes BIPA's requirements and the potential liability for companies, some of the most noteworthy cases and settlements, the most common and effective defenses against these types of lawsuits, and how companies can protect themselves against potential liability.

WHAT IS THE POTENTIAL BIPA LIABILITY FOR COMPANIES?

BIPA requires that any private entity that collects biometric identifiers and information:

- Develop a written policy with retention schedule and guidelines;
- Provide written notice;
- Obtain informed consent;
- Refrain from dissemination; and
- Adequately protect the information collected.

* Michael G. Babbitt, a partner in the Litigation and Intellectual Property Departments of Willkie Farr & Gallagher LLP, focuses his practice on complex civil litigation and counseling involving patents and technology. J. Mylan Traylor is an associate in the firm's Litigation Department. Resident in the firm's office in Chicago, the authors may be contacted at mbabbitt@willkie.com and mtraylor@willkie.com, respectively.

BIPA includes a private right of action that enables any person aggrieved to recover for each violation, liquidated damages of $1,000 or actual damages (whichever is greater) for negligent violations, and liquidated damages of up to $5,000 or actual damages (whichever is greater) for intentional or reckless violations, plus attorneys' fees and costs, and injunctive relief.

For years, employers and other businesses of varying types and sizes, have become targets of BIPA class actions. The bulk of those lawsuits have accused employers of failing to abide by notice and consent provisions embedded in the law, before they require workers to scan fingerprints or some other biometric identifier to verify their identity when punching the clock at job sites, or when accessing secure facilities. When multiplied across an entire workforce or customer base, improperly scanning prints or collecting other biometric information several times a day, for years, the potential payout can climb into the millions of dollars.

Many other states have enacted and considered privacy laws that are very similar if not substantially the same as BIPA, such as Texas,[1] Washington,[2] California[3] and Arkansas.[4] Indeed, at least 27 other states have introduced some form of biometrics legislation.[5] As such, companies should consider the requirements of BIPA even if they do not operate within the purview of BIPA.

RECENT SETTLEMENTS

The settlement values in BIPA cases vary widely, and depending on the facts of each case; however, one thing is clear: both the number of public BIPA class settlements and the corresponding dollar amounts continue to rise.

In February 2022, Kronos Inc. agreed to pay nearly $15.3 million to end a lawsuit accusing it of violating BIPA by improperly collecting and storing the fingerprints or palm prints of workers at companies that use Kronos' biometric timekeeping devices.

---

[1] Tex. Bus. & Com. Code § 503.001.

[2] Wash. Rev. Code Ann. § 19.375.020.

[3] CA Civ. § 1798.100 et seq.

[4] Arkansas Code § 4-110-103(7).

[5] 2021 AL H.B. 216 (Alabama); 2021 AK S.B. 116 (Alaska); 2021 CO H.B. 1244, S.B. 190 (Colorado); 2021 CT S.B. 893 (Connecticut); 2021 FL H.B. 969 (Florida); 2021 HI S.B. 1009 (Hawaii); 2020 IN H.B. 1371 (Indiana); 2021 KY S.B. 280 § 2(5), 2022 KY H.B. 32 (Kentucky); 2021 ME S.P. 535 (Maine); 2021 MD S.B. 16, 2022 MD H.B. 259 (Maryland); 2021 SD. 1726, 2022 S.2667 (Massachusetts); 2021 MS S.B. 2612 (Mississippi); 2022 MO H.B. 2716 (Missouri); 2021 MN S.F. 1408 (Minnesota); 2021 MT H.B. 710 (Montana); 2020 NJ A.B. 3625 (New Jersey); 2021 NY A.B. 27 (New York); 2021 NC S.B. 569 (North Carolina); 2021 OK H.B. 1602 (Oklahoma); 2021 PA H.B. 5945 (Pennsylvania); 2019 RI H.B. 5945, 2019 RI S.B. 234 (Rhode Island); 2021 SC H.B. 3063 (South Carolina); 2021 UT S.B. 200 (Utah); 2020 VA H.B. 2307 (Virginia); 2021 WV H.B. 2064, 2021 WV H.B. 3159 (West Virginia); 2019 WI S.B. 851 (Wisconsin).

The complaint accuses Kronos of failing to inform employees why or for how long their sensitive personal data is being collected or stored, and that until recently, Kronos had not published a written policy containing a data retention schedule or guidelines for permanently destroying that biometric information. Plaintiffs also claimed that Kronos profits from the use of employees' biometric data, as it markets its biometric products as superior options to traditional time clocks. The case is *Figueroa, et al. v. Kronos Inc*.[6]

In November 2021, a $50 million dollar class action settlement was given preliminary court approval. The lawsuit was filed against McDonald's and several affiliates. The lawsuit alleges that McDonald's restaurants in Illinois collected employee biometric information upon clocking without providing the required disclosures or obtaining consent under BIPA. The cases are *Lark, et al. v. McDonald's USA LLC, et al.*,[7] and *Arthur, et al., v. McDonald's USA LLC, et al*.[8]

In June 2021, an Illinois trial court granted final approval of a class action settlement for $10 million in the lawsuit *Roach v. Walmart, Inc.*[9] The class action involves claims that the company violated the BIPA by requiring workers to scan handprints without obtaining their consent.[10]

Indeed, last year, a major social media company paid $650 million to resolve allegations that it stored digital scans of users' faces in violation of BIPA. Other recent settlements include a $2.6 million settlement with Top Golf USA Inc. and a $1 million settlement with Lifespace Communities Inc., both of which resolved claims that workers' fingerprints were collected without their consent.

RECENT UPDATES SURROUNDING COMMON LEGAL DEFENSES

The Workers Compensation Act

Recently, many companies have attempted to argue that BIPA claims cannot proceed in court, because they are preempted by Illinois' Workers' Compensation Act ("IWCA"), which they claim provides the exclusive remedy for injuries that occur in the workplace. On February 3, 2022, the Illinois Supreme Court unanimously ruled in *McDonald v. Symphony Bronzeville Park LLC*[11] that the exclusivity provisions of the state's workers' compensation statute do not preclude liquidated damages claims under BIPA.

---

[6] *Figueroa, et al. v. Kronos Inc.*, Case No. 1:19-cv-01306 (N.D. Ill.).

[7] *Lark, et al. v. McDonald's USA LLC, et al.*, Case No. 17-L-559 (Cir. Ct. Ill.).

[8] *Arthur, et al., v. McDonald's USA LLC, et al.*, Case No. 20-L-0891 (Cir. Ct. Ill.).

[9] *Roach v. Walmart, Inc.*, Case No. 2019-CH-01107 (Cir. Ct. Ill.).

[10] *See also Bryant, et al. v. Compass Group*, Case No. 19-CV-6622 (N.D. Ill. Nov. 2, 2021) (preliminary settlement approval for $6.8 million sought for a class action involving claims that the company violated BIPA by collecting fingerprint data without the consent of their workers).

[11] *McDonald v. Symphony Bronzeville Park LLC,* Case No. 2022-IL 126511 (Ill. Feb. 3, 2022).

The decision is a blow to employer defendants that sought to argue that the IWCA provided the exclusive remedy for an employee's claims against their employer, and that these sorts of class actions should be removed from court, because the alleged injury suffered by the workers under BIPA occurred in the workplace. In *McDonald*, the Illinois Supreme Court did agree that IWCA typically provides the exclusive remedy for employees' claims against their employers, but held that the class could nonetheless pursue their BIPA claims "in the circuit court, rather than through a claim before the Workers' Compensation Commission, because McDonald's and the putative class's alleged injury is not one that 'categorically fits within the purview of the [Compensation] Act.'" The court noted that the workplace injuries suffered by workers who have had their biometric information collected and stored, without consent and without first receiving the notices required by BIPA are not the same as a typical physical or mental injury that would be covered by the IWCA.

As such, this IWCA preemption theory is no longer a viable argument for companies defending BIPA claims.

Statute of Limitations

One commonly used defense in BIPA cases is that plaintiffs' claims are untimely. BIPA itself does not provide a statute of limitations, and so, for years, the question of which statute of limitations applies to BIPA cases had not been answered. On September 17, 2021, the Illinois appellate court held that a one-year statute of limitations applies to causes of action alleging violations under Sections 15(c) and (d) of the Illinois Biometric Information Privacy Act (BIPA),[12] while a five-year limitations period applies to those alleging violations of Sections 15(a), (b) and (e).

In *Tims v. Black Horse Carriers, Inc.*, the First District considered whether the limitations period in 735 ILCS 5/13-201 (governing privacy claims) or the limitations period in 735 ILCS 5/13-205 (a catch-all provision) applies. Section 13-201 establishes a one-year limitation period for actions for "slander, libel or for publication of matter violating the right of privacy." By contrast, Section 13-205 provides a catch-all limitations period of five years for, in relevant part, "all civil actions not otherwise provided for" by statute.

The *Tims* court held that the one-year limitations period applies to actions brought pursuant to Sections 15(c) and (d) of BIPA, while the five-year limitations period applies to those brought under Sections 15(a), (b) and (e). Sections 15(c) and 15(d) govern the sale and disclosure of biometric data. Section 15(a) governs written policies on and the destruction of biometric data, and Sections 15(b) and (e) govern the collection and storage of biometric data.

[12] 740 ILCS 14/1 et seq.

Thus, some of the most common BIPA claims, claims for failure to maintain and comply with a publicly available retention policy (Section 15(a)), and to provide written notice and receive written consent (Section 15(b)), are granted a longer limitations period of five years, as opposed to inappropriate disclosure claims under Sections 15(c) and (d), which must be brought within one year.

It is worth noting that the *Tims* decision is likely not the last word on the issue. On January 26, 2022, the Illinois Supreme Court granted a petition for leave to appeal this case. As such, the Illinois Supreme Court might soon provide a final answer on the applicable statute of limitations for BIPA claims.

Relatedly, the question of when and how many times a BIPA claim accrues is still unanswered. The Illinois Supreme Court has yet to define what constitutes a "collection" of biometric information and so it is unclear whether claims accrue each time a company collects biometric data or only the first instance. This question is of paramount importance for determining damages. Acting on a certified question from the U.S. Court of Appeals for the Seventh Circuit in *Cothron v. White Castle System, Inc.*,[13] the court will decide whether BIPA claims accrue only once upon the initial collection or disclosure of biometric information, or each time biometric information is collected or disclosed.

Lack of Jurisdiction

Although BIPA is an Illinois statute, its effect often reaches far beyond the state, implicating out-of-state defendants with no Illinois operations. While courts have held that the Act does not apply extraterritorially, courts must perform a personal jurisdiction analysis to determine whether Illinois courts have jurisdiction over a defendant. Courts have general jurisdiction where a defendant has continuous and systematic affiliations with Illinois to render a defendant essentially at home in the state and specific jurisdiction if there is sufficient affiliation between Illinois and the underlying controversy.

A corporation not based in Illinois may try to argue that it does not have sufficient contacts with the state to be subject to the jurisdiction of Illinois courts. Some courts have indeed dismissed BIPA suits for lack of personal jurisdiction due to a defendant's lack of contacts with Illinois.[14] However, courts dismissing BIPA cases based on a lack of specific jurisdiction is rare. Most BIPA suits are brought against either an employer with substantial operations in Illinois or a consumer-facing company who uses biometrics and sufficiently targets Illinois consumers, both of which may be sufficient to establish a court's personal jurisdiction over a defendant.

---

[13] *Cothron v. White Castle System, Inc.*, 20 F.4th 1156 (7th Cir. 2021).

[14] *See, e.g., Bray v. Lathem Time Co.*, No. 19-3157 (C.D. Ill. Mar. 27, 2020) (holding that the "random and attenuated nature" of a defendant's contacts with Illinois did not amount to sufficient contacts with Illinois to warrant the exercise of specific jurisdiction).

HOW COMPANIES CAN BEST PROTECT THEMSELVES

The best defense against a BIPA claim is, of course, compliance with the statute. Companies should implement the following steps to ensure they do not run afoul of BIPA:

- Provide clear advanced written notice to individuals that their biometric data will be collected and stored. Ensure that the notice adequately discloses why the data is being collected, how it will be used, how it will be stored, and whether and how it will be disclosed. Many companies provide notice in the form of a pop-up message that appears each time before a user or employee has their data collected. This kind of notice can be provided in other ways too. Companies can also include a notice of biometric policies in their terms and conditions and privacy policies.

- Obtain written consent. Before the collection or use of the biometric data, companies should obtain written consent for the collection, storage, and use of a user's biometric data. This can be done by requiring employees to sign a form authorizing the collection of the biometric data, or in the consumer context, requiring users to tap or click "yes" to a consent prompt. Companies can also allow individuals to opt out of biometric information collection. Finally, companies often keep records of users' written consent for as long as the data is stored.

- Create a data retention policy. This policy should inform employees or users when their biometric data will be destroyed. The policy should explain that the data will be destroyed when the purpose for the data's collection has been achieved, or within three years, whichever occurs sooner.

- Consider an appropriate data retention system. Companies may use a system or database that handles the flow of biometric data from collection to storage, use, and destruction. Companies may document this flow of information for each user so that there are records in the event of a lawsuit. BIPA requires an employer to store, transmit, and protect this data in a reasonable standard of care within the employer's industry, and in a way that is at least as protective as the company's own confidential or sensitive information. Both of these standards leave room for interpretation and so it is recommended that employers seek the advice of an attorney and IT professionals to comply with these standards. In particular, in some cases, the technical details of how and when the data is stored may become an issue, and it may be useful to have a team with computer software and programming knowledge.

- Consider whether use of biometric technology is even necessary. For many companies, there may be alternative methods to accomplishing their goals without collecting biometric information (e.g., using an employee pin clock-in system as opposed to scanning fingerprints). Until there is a decrease in the number of these lawsuits and or the potential liability for companies, it might be prudent to avoid the issue all together if the use of biometric information is not necessary for a company or product to function. However, for other companies, biometric technology may be vital to the business, and in such cases, compliance efforts may become important.