JOURNAL OF EMERGING ISSUES IN LITIGATION

Tom Hagy
Editor-in-Chief

Volume 2, Number 3
Summer 2022

Editor's Note
Tom Hagy

The "Ending Forced Arbitration of Sexual Assault and Sexual Harassment Act of 2021" Finally Levels the Playing Field
Kathryn V. Hatfield

Workplace Investigations: Proactive Assessments Mitigate the Risk of Costly Litigation in a Newly Remote Environment
Stefani C Schwartz

Taking the High Ground: Where Cannabis Insurance Litigation is Trending (and Why)
John B. McDonald

Asymmetrical Combat: Bad Faith Liability in Insurance Recovery Cases
William G. Passannante

Wildfire Claims and Coverage
Scott P. DeVries and Yosef Y. Itkin

Biometric Privacy Laws: Companies Will Need Insurance as Protection from New and Expanding Liability
Cort T. Malone and Jade W. Sobh

fastcase FULL COURT PRESS

Journal of Emerging Issues in Litigation

Volume 2, No. 3 Summer 2022

175 Editor's Note
Tom Hagy

179 The "Ending Forced Arbitration of Sexual Assault and Sexual Harassment Act of 2021" Finally Levels the Playing Field
Kathryn V. Hatfield

187 Workplace Investigations: Proactive Assessments Mitigate the Risk of Costly Litigation in a Newly Remote Environment
Stefani C Schwartz

195 Taking the High Ground: Where Cannabis Insurance Litigation is Trending (and Why)
John B. McDonald

201 Asymmetrical Combat: Bad Faith Liability in Insurance Recovery Cases
William G. Passannante

213 Wildfire Claims and Coverage
Scott P. DeVries and Yosef Y. Itkin

235 Biometric Privacy Laws: Companies Will Need Insurance as Protection from New and Expanding Liability
Cort T. Malone and Jade W. Sobh

JOURNAL OF EMERGING ISSUES IN LITIGATION at $395.00 annually is published four times per year by Full Court Press, a Fastcase, Inc., imprint. For customer support, please contact Fastcase, Inc., 711 D St. NW, Suite 200, Washington, D.C. 20004, 202.999.4777 (phone), 202.521.3462 (fax), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Morgan Morrissette Wright
Production Editor: Sharon D. Ray
Cover Art Design: Morgan Morrissette Wright and Sharon D. Ray

Cite this publication as:

Journal of Emerging Issues in Litigation (Fastcase)

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

711 D St. NW, Suite 200, Washington, D.C. 20004
https://www.fastcase.com/

POSTMASTER: Send address changes to JOURNAL OF EMERGING ISSUES IN LITIGATION, 711 D St. NW, Suite 200, Washington, D.C. 20004.

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Tom Hagy, Editor-in-Chief, tom.hagy@litigationconferences.com

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. 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.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

Morgan Morrissette Wright, Publisher, Full Court Press at mwright@fastcase.com or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service
Available 8am–8pm Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)

Biometric Privacy Laws: Companies Will Need Insurance as Protection From New and Expanding Liability

Cort T. Malone and Jade W. Sobh*

Abstract: *As more states follow Illinois in enacting biometric privacy laws, the risk that companies will be hit with lawsuits and extensive damages awards increases. Employers are among the most active collectors of this type of data, collecting fingerprints and deploying facial recognition for timekeeping and security purposes. Several multi-million dollar settlements have been reported for violations of biometric privacy laws. Meta, formerly Facebook, paid $650 million to resolve claims that it improperly stored face scans of its users. When companies turn to their insurance carriers, policyholders have a good track record of receiving coverage. Now that these claims are becoming more prevalent, will the insurance industry work to limit its exposure in this space? What should policyholders do in the event the industry is successful? In this article, the authors provide background on these emerging privacy laws, how they have played out in court, and what types of policies companies should consider to be sure they have the necessary protection.*

At least seven states have passed biometric privacy laws specifically intended to protect individuals from the collection, use, and sale of their personal biometric identifiable information. Several of these laws allow for extensive damages awards regardless of whether individuals suffered any actual harm as a result of the nonconsensual collection of biometric data. The companies facing class action lawsuits as a result should look to insurance to cover such claims, as the initial litigation with insurance companies has

Journal of Emerging Issues in Litigation / Summer 2022, Vol. 2, No. 3, pp. 235–243.

provided favorable results to policyholders. But insurance companies surely will seek to limit future exposure related to biometric privacy law violations, and companies either using biometrics or potentially doing so in the future would be wise to seek and maintain the broadest possible coverage.

A Primer on Biometric Data

Biometric Identifiable Information (BII) is generally defined as any physiological or biological characteristic that is used by or on behalf of a commercial establishment to identify an individual. BII may take the form of a retina scan, a fingerprint, a voiceprint, a scan of hand or face geometry, or any other identifying characteristic. BII is a more secure, reliable, and convenient form of identification—as opposed to passwords or account information—as you cannot forget or share your biometric identifiers; however, with the added convenience comes added risk, because your BII cannot be replaced or changed if stolen. Businesses may use BII for punch cards, airport security, access to buildings or technology, or even for biometric marketing. The increased use of BII has predictably led to state regulation to protect consumers' and employees' biometric data.

Current and Proposed Biometric Protection Laws

One of the most consumer friendly Biometric Privacy Laws is the Illinois Biometric Information Privacy Act (BIPA), but other states have also enacted Biometric Privacy laws, including Texas, Washington, California, New York, Virginia, and Arkansas.

BIPA, enacted in Illinois in 2008, was one of the first state laws to address business's collection of biometric data. BIPA requires companies to acquire informed consent prior to collection, permits a limited right to disclosure, mandates protection obligations and retention guidelines, and prohibits profiting from biometric data. Critically, BIPA creates a private right of action for individuals harmed by BIPA provisions and provides statutory damages of up to $1,000 for each negligent violation, and up to $5,000 for each

intentional or reckless violation. In 2019, the Illinois Supreme Court decided that actual harm is not required to establish standing to sue under BIPA. *See Rosenbach v. Six Flags Entertainment Corp.*, No. 123186 (Ill. 2019). Now, any time an organization violates even a technical or procedural aspect of BIPA, even in the absence of specific injury or adverse effect, the individual whose biometric data was collected has standing to sue under the Act. BIPA has resulted in some of the largest settlements of all the BII privacy laws and surely will continue to produce large class-action cases and sizable settlements.

Following BIPA's enactment in 2008, Texas passed the Capture or Use of Biometric Identifier Law (CUBI), which imposes similar requirements relating to notice, consent, prohibitions on disclosures, and mandatory data security measures. Significantly, CUBI imposes penalties of up to $25,000 per violation with no maximum cap, but unlike in Illinois, the power to enforce CUBI rests exclusively with the Texas Attorney General.

In 2017, Washington State followed suit to become the third state to enact a targeted biometric privacy law: the Biometric Identifiers Law (BIL). The BIL is more narrowly tailored than BIPA or CUBI, as it does not require affirmative consent for the collection, use, or disclosure of biometric data, but rather only restricts the "enrollment" of biometric identifiers into a database for commercial purposes and further sale or disclosure of those enrolled identifiers. Under BIL, a person or company "may not enroll a biometric identifier in a database for a commercial purpose without first providing notice, obtaining consent, or providing a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose." Only after a biometric identifier has been enrolled in a database does BIL prohibit selling, leasing, or disclosing it without individual consent. Like in Texas, only the Washington Attorney General may enforce the law's requirements.

In 2018, California passed the California Consumer Privacy Act (CCPA), which expanded its existing privacy and information security regulatory framework to cover biometric data. The CCPA covers an employer's collection of data for applicants and employees, and applies to companies doing business in California that (1) have at least $25 million of annual gross revenues; (2) buy,

receive, share, or sell the personal information of more than 50,000 consumers, households, or devices for commercial purposes; or (3) receive 50% or more of their annual revenues from selling consumers' personal information. The law requires covered businesses to provide certain notices to consumers or employees about the type of information that is collected and how the business uses the information. The law also requires that the consumer be able to request a copy of the personal information collected, and to request that the data be deleted. The CCPA is enforced by the California Attorney General.

On July 9, 2021, New York City's Biometric Identifier Information Law (BII Law) went into effect. The BII Law bans the sale of biometric data and imposes notice requirements on covered businesses that use biometric identifying technology in their establishments. While comparisons have been made to BIPA, New York City's new BII Law—which provides a cure period for certain violations and permits collection of biometric data without written consent—is far less stringent and is not expected to produce the maelstrom of litigation precipitated by BIPA. That said, policyholders still should be aware of the BII Law's requirements and consider potential insurance coverage implications. Under the BII Law, businesses may not sell, lease, share for value, or otherwise profit from the transmission of biometric identifier information, and covered businesses that collect, retain, convert, store, or share biometric identifier information must post conspicuous signage at all customer entrances disclosing that such information is being collected.

Like BIPA, the BII Law provides a private right of action to parties "aggrieved" by violations but includes a 30-day cure period for businesses accused of violating the posting requirement. Further, any party alleging a posting violation must provide written notice to the business before bringing its claim. Importantly, however, written notice is not required before bringing claims for the illegal sale or sharing of biometric information, and there is no cure period for such claims. Prevailing claimants can recover $500 per posting violation, $500 per negligent selling violation, and $5,000 per intentional or reckless selling violation.

Noteworthy Disputes and Settlements

Since the enactment of biometric privacy laws there have been many notable disputes and staggering settlements. Last year, a California Federal Judge approved a $650 million settlement resolving claims that Facebook's facial recognition technology violated Illinois users' biometric privacy rights under BIPA. There have been several other notable BIPA settlements, including a $25 million class action settlement to end a putative class action brought against technology company ADP concerning its provision of biometric scanning technology to employers for timekeeping purposes. The parties to the seminal Six Flags litigation received preliminary approval for a proposed class action settlement with an anticipated value of $36 million. *See Rosenbach v. Six Flags Ent. Corp.,* 129 N.E.3d 1197 (Ill. 2019). Compass Group USA Inc. and a retail technology company agreed to pay $6.8 million as part of a settlement to resolve claims alleging that they collected fingerprint data from vending machine users without proper notice and consent as required under BIPA. And a federal court in Illinois granted preliminary approval to a $92 million settlement reached in the TikTok multidistrict litigation—accusing the company of collecting and sharing biometrics and location data from users—over objections that had been raised concerning the basis and terms of settlement.

Recently, the Texas Attorney General brought suit against Meta, the parent Company of Facebook and Instagram, over the company's collection and use of biometric data. The suit alleges that Meta collected and used Texans' facial geometry data in violation of the Texas CUBI and the Texas Deceptive Trade Practices Act (DTPA). The lawsuit is significant because it represents the first time the Texas Attorney General's Office has brought suit under CUBI and may provide a road map for other states. As stated earlier, the fine for each violation is $25,000, and the Attorney General alleges that Facebook repeatedly captured Texans' biometric identifiers without their consent on literally billions of separate occasions, all in violation of CUBI and DTPA.

Different Types of Insurance Policies Potentially Offer Protection to Companies

Businesses may look to various types of insurance policies for protection from the sudden and ever-increasing liability under present and soon to pass biometric data privacy laws, including commercial general liability insurance, employment practices liability insurance, cyber insurance, and directors & officers (D&O) insurance.

General liability policies may provide some degree of protection from biometric liability. In *West Bend Mutual Ins. Co. v. Krishna Schaumburg Tan*, a policyholder sought coverage under the policy provision providing coverage for liability arising out of "written publication of material that violates a person's right of privacy." 2020 IL App (1st) 191834, 166 N.E.3d 818, *appeal allowed*, 154 N.E.3d 804 (Ill. 2020), and *aff'd*, 2021 IL 125978. The policyholder had provided customers' fingerprint data to a vendor. The insurance company argued that no "publication had occurred because that term required dissemination to a wide audience," but the court disagreed, holding that "publication was also commonly understood to encompass more limited sharing with a single party." The court ultimately found in favor of the policyholder.

Similarly, in *Citizens Insurance Company of America v. Thermoflex Waukegan*, a policyholder argued that two insurance companies were obligated to defend Thermoflex under their commercial lines insurance policy, which provided coverage for "personal and advertising injury." The insurance companies argued that they were shielded by a policy exclusion—an "access or disclosure" exclusion—barring coverage for any personal or advertising injury arising out of any access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information, or any other type of nonpublic information. 20-cv-05980 (N.D. Ill. Mar. 1, 2022). The court denied the insurance companies' motion for judgment on the pleadings as to this exclusion, finding that it was at best unclear, as handprints do not share the same attributes as the types of information enumerated above. The court also rejected the insurance

company's attempts to apply two other coverage exclusions, one excluding coverage for certain employment practices and the other excluding coverage for liability incurred for collection or dissemination of information under laws akin to the Telephone Consumer Protection Act (TCPA). The court found application of each of these exclusions to BIPA liability overly broad, requiring ruling in favor of the policyholder.

Some courts have applied employment practices liability insurance (EPLI) to BII coverage lawsuits. In *Twin City Fire Ins. Co. v. Vonachen Servs. Inc.*, the U.S. District Court for the Central District of Illinois held that an EPLI policy provided coverage to an employer defending against allegations that its timekeeping system violates BIPA. No. 20-CV-1150-JES-JEH, 2021 WL 4876943 (C.D. Ill. Oct. 19, 2021). The court held that allegations by employees that they were required, as a condition of employment set forth in the company handbook, to use the fingerprint-based timekeeping system potentially brought the underlying claim within that scope of EPLI coverage. The EPLI coverage also covered claims alleging "an employment-related invasion of privacy, including without limitation, an Employee Data Privacy Wrongful Act," which the court held included alleged violations of BIPA.

D&O insurance also may apply to biometric claims in certain situations. Public company D&O policies typically provide coverage to the entity for securities claims, which could include claims that, for example, the company failed to disclose in its SEC filings that it was subject to potential liability for biometric violations. Public company D&O policies also should apply to cover directors and officers facing lawsuits arising from company biometric violations. Such a suit might allege that the value of company stock fell because of biometric violations, and that the directors and officers failed to oversee corporate operations that resulted in the biometric violations. Private company D&O policies also provide entity coverage that conceivably covers biometric claims. In one case where D&O coverage was sought, the *Vonachen Services* litigation mentioned above, the court held that an invasion of privacy exclusion barred D&O coverage because the exclusion precluded coverage for loss "in connection with any claim based upon, arising from, or in any way related to any actual or alleged [. . .] invasion of privacy." *Id.*

Despite this holding, both public and private company policyholders should investigate D&O coverage, and the corresponding exclusions, should they be faced with biometric claims.

Lastly, cyber insurance may be another method of obtaining coverage for biometric privacy law liability. The cyber insurance marketplace has more than doubled in the past five years. Cyber insurance is becoming common practice, although several insurance companies have started to sublimit or exclude coverages in order to maintain profitable books of cyber business. Other insurance companies have exited the cyber marketplace altogether as claims continue to rise in frequency and severity. Recently, in *Citizens Ins. Co. of America v. Superior Knife LLC*, a policyholder and insurance company argued over the extent of coverage within a cyber liability provision, and the application of certain exclusions that might bar coverage. No. 1:21-cv-06586 (N.D. Ill. Dec. 9, 2021). Specifically, the insurance company argued that exclusions, including personal or advertising injury arising out of employment-related practices and policies, unlawful recording and distribution of material, and access or disclosure of confidential personal information, may bar coverage for the policyholder—similar to the argument that insurance companies made in *Thermoflex*, where the court found for the policyholder.

The main takeaway from these cases is that companies should be examining their insurance policies now in light of the expanding universe of biometric privacy laws. Both the use of biometrics and the proliferation of privacy laws to protect against such use will only continue to grow. Locking in favorable policy terms to secure insurance coverage to defend litigation over these issues is critical to a company's ability respond to these inevitable claims.

Conclusion

The increased collection, storage, sharing, and sale of BII, alongside the increase in regulation of BII means that companies must look to their insurance policies for protection when faced with claims under biometric privacy laws. As different statutes may be more consumer friendly than others, and certain districts may be less willing to side with policyholders in coverage disputes,

it is critical that companies take these risks seriously, and consult with knowledgeable risk managers and attorneys when considering how their use of biometric data will impact the present and future of their business.

Note

* Cort T. Malone (cmalone@andersonkill.com) is a shareholder in the New York and Stamford offices of Anderson Kill and practices in the Insurance Recovery and the Corporate and Commercial Litigation Departments. He represents policyholders in insurance coverage litigation and dispute resolution, with an emphasis on commercial general liability insurance, directors and officers insurance, employment practices liability insurance, advertising injury insurance, and property insurance issues. Jade W. Sobh (jsobh@andersonkill.com) is an attorney in Anderson Kill's New York office. Jade focuses his practice on insurance recovery, exclusively on behalf of policyholders, as well as regulatory and complex commercial litigation matters.