ABA

COMPANIES, BEWARE: EMAILS ARE FOREVER

BAD CLIENTS AND WHAT TO DO ABOUT THEM

IN FEDERAL COURT, NEVER, EVER...

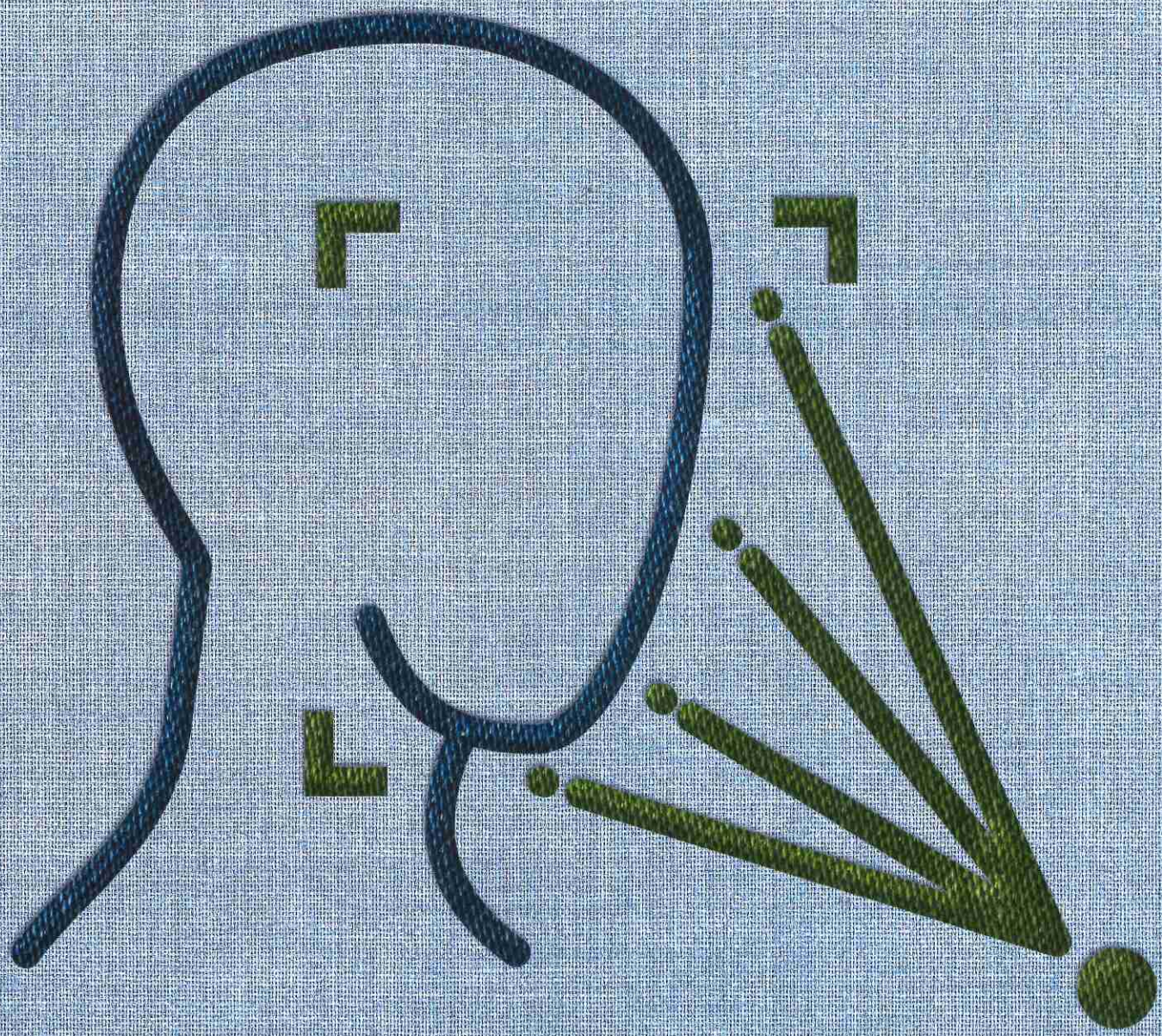
VOL 44 NO 4
SUMMER 2019

LITIGATION NEWS

A PUBLICATION OF THE AMERICAN BAR ASSOCIATION | SECTION OF LITIGATION

GROWING PATCHWORK OF BIOMETRIC PRIVACY LAWS

By Kristen L. Burge,
Litigation News Associate Editor



Growing Patchwork of Biometric Privacy Laws

Court lowers bar for standing, interpreting "aggrieved person" broadly

Fingerprints, retinal scans, and facial recognition software offer additional security measures and efficiency for consumers. But unlike a password or barcode, biometric identifiers cannot be changed in the event of a breach. As businesses gravitate toward biometrics, states grapple with how best to protect individuals' biometric privacy. Illinois was the first to enact a comprehensive framework regulating the collection, use, storage, and disclosure of biometric information—the Biometric Information Protection Act (BIPA). To date, it is also the only biometric privacy statute to grant "aggrieved persons" a private cause of action. That, in turn, has raised questions regarding whether the law applies to individuals and companies outside the state, and whether plaintiffs must show actual harm from the statutory violation—often a key point of contention in privacy suits generally.

In *Rosenbach v. Six Flags Entertainment Corporation*, the Illinois Supreme Court resolved the unanswered question of whether an "aggrieved person" must also suffer an actual injury to have standing to bring a BIPA claim. By holding that BIPA does not require actual harm for standing, *Rosenbach* appears to depart from federal case law, which requires a plaintiff to demonstrate an "injury-in-fact" for Article III standing. The decision also may lead to more litigation over technical violations that otherwise would have faltered at the pleading stage, according to ABA Section of Litigation leaders. Given the potential for increased liability exposure, Section of Litigation leaders advise companies to evaluate their operational and legal practices to ensure compliance with evolving privacy laws.

What Is BIPA Anyway?

BIPA applies to all biometric identifiers, which are defined as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." It excludes "writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color."

Under BIPA, any "private entity" that collects, stores, or uses biometric information in Illinois—regardless how it is collected, stored, or used, or for what reason—must:

- Establish a written policy with a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information;
- Notify individuals in writing that the information is being collected or stored, and the purpose and length of time for which the biometric identifier will be collected, stored, and used;
- Obtain a written release from the individual; and
- Not disclose biometric information to a third party without the individual's consent.

While BIPA defines "written release" as "informed written consent or, in the context of employment, a release executed by an employee as a condition of employment," it does not elaborate on how extensive the release or consent must be to comply.

Finally, BIPA requires a company to use "the reasonable standard of care" within its industry for storing, transmitting, and protecting biometric information and act "in a manner that is the same as or more protective than the manner in which the [company] stores, transmits and protects other confidential and sensitive information."

Courts would often dismiss cases brought before *Rosenbach* because the plaintiff failed to allege actual damages. As a result, many issues have not yet been litigated.

Failing to comply with any of the foregoing requirements subjects a company to a lawsuit by "[a]ny person aggrieved by a violation of this Act." Notably, BIPA does not define "aggrieved" or "person aggrieved." Remedies include monetary damages, injunctive relief, attorney fees, and any other relief the court deems appropriate. A negligent violation warrants $1,000 in statutory damages or actual damages, whichever is higher, whereas the liquidated damages for a reckless or intentional violation garners $5,000 per violation.

Challenging Standing to Sue

In *Rosenbach*, the defendant Six Flags obtained fingerprints when issuing season passes to reduce fraud and streamline admissions to its amusement parks. On subsequent visits, pass holders would scan their fingerprints to enter and exit the amusement park. The plaintiff purchased a season pass online for her 14-year-old son to use on his class trip and provided her son's personal information. When the plaintiff's son arrived at the park, Six Flags required him to scan his fingerprint into the biometric data capture system before issuing his physical pass.

The plaintiff sued Six Flags for violating BIPA, alleging the park failed to inform her "in writing (or in any other way) of the specific purpose and length of term for which his fingerprint was being collected, stored and used," and failed to get her written consent to collect, store, sell, or disclose her son's fingerprint. The plaintiff further alleged the park did not publish the required written policy on its "retention schedule or guidelines for retaining and then permanently destroying biometric identifiers and biometric information." She sought statutory damages, injunctive relief, and restitution of money paid for the pass, but not actual damages.

Six Flags moved to dismiss, arguing that in the absence of actual damages, the plaintiff was not an "aggrieved person" under BIPA and therefore lacked standing to sue. The trial court denied Six Flags's motion as to the BIPA claim but certified for interlocutory appeal the issue of whether an "aggrieved person" included persons alleging only a technical violation of the statute, with no actual injury—an issue of first impression.

On appeal, the Illinois Appellate Court held that a person alleging a "technical violation of the Act" without alleging any injury or adverse effect is not an "aggrieved" person. A person must allege actual—though not necessarily pecuniary—damages to be considered "aggrieved." Because

Photo Illustration: Elmarie C. Jara © Getty Images

the plaintiff did not allege actual damages, the appellate court concluded she could not maintain her action against the amusement park.

Broad Interpretation of "Aggrieved" Paves the Way for Additional Lawsuits

A unanimous Illinois Supreme Court reversed the appellate court and remanded the matter to the trial court. In so holding, the *Rosenbach* court relied on a long-standing precedent interpreting "aggrieved" as "a substantial grievance; a denial of some personal or property right." It also cited prior interpretations of the term, noting that "[a] person is prejudiced or aggrieved, in the legal sense, when a legal right is invaded by the act complained of *or* his pecuniary interest is directly affected by the decree or judgment." The court presumed, given the term's enduring meaning, that the legislature was aware of the precedent and acted with the term's prior use in mind.

Based on that precedent, the Illinois Supreme Court held that the appellate court erred in characterizing the park's violations as "merely technical" because it "misapprehends the nature of the harm our legislature is attempting to combat through this legislation." According to the *Rosenbach* court, "[w]hen a private entity fails to adhere to the statutory procedures, as defendants are alleged to have done here, the right of the individual to maintain [his or] her biometric privacy vanishes into thin air." Thus, the "precise harm the Illinois legislature sought to prevent is then realized. This is no mere 'technicality.' The injury is real and significant." Accordingly, it concluded that a showing of actual harm is not necessary to establish a claim for violation of BIPA.

Decision Clarifies BIPA, but Ambiguities Remain

Biometric information's prevalence in the marketplace and emerging law in the area makes *Rosenbach* "a fascinating case," remarks Elizabeth "Lisa" B. Vandesteeg, Chicago, IL, cochair of the Membership Subcommittee of the Section's Privacy & Data Security Committee. "We will likely see a substantial uptick in class action lawsuits following this decision. Indeed, the plaintiffs' bar will be excited to know statutory violations are sufficient to bring a cause of action. Certainly, as a matter of public policy, this seems to be what the general assembly intended," surmises Vandesteeg.

Though *Rosenbach* "resolves one of the biggest outstanding issues on statutory interpretations for BIPA," several issues regarding BIPA's provisions are ripe for litigation, according to Alexander "Sandy" R. Bilus, Philadelphia, PA, cochair of the Section's Privacy & Data Security Committee. "Courts would often dismiss cases brought before *Rosenbach* because the plaintiff failed to allege actual damages. As a result, many issues have not yet been litigated," Bilus explains. "It is still up in the air as to how specific consent must be and whether a type of click-through agreement is adequate," he adds. "To the best of my knowledge, the question of what BIPA requires for 'informed written consent' has not been identified or challenged yet," agrees Vandesteeg. Section leaders also anticipate litigation over what constitutes negligent versus reckless or intentional conduct in the biometric privacy space.

While BIPA applies to transactions that occur within Illinois, there is no specific formula or bright-line test for determining whether a transaction occurs in the state. According to the Illinois Supreme Court, "a court must analyze whether 'the circumstances relating to the transaction occur primarily and substantially' within Illinois." Because this inquiry is so fact and technology driven, "we can expect to see litigation over how BIPA applies to companies operating outside of Illinois but arguably collecting data within the state," predicts Bilus. For example, California courts are grappling with how to apply BIPA to tech companies that use facial recognition software to collect biometric information of Illinois residents, Bilus notes. Particularly difficult is determining whether cloud or internet activity "primarily and substantially" takes place in Illinois, he adds.

Section leaders also anticipate Article III standing challenges in federal court. While *Rosenbach* makes it clear that BIPA claimants can sue in *state* court without alleging actual harm, Section leaders question whether federal courts will arrive at the same conclusion for federal standing. As the U.S. Supreme Court explained in *Spokeo, Inc. v. Robins*, "standing requires a concrete injury even in the context of a statutory violation," and, therefore, a plaintiff "could not . . . allege a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement." The Court acknowledged "[t]his does not mean, however, that the risk of real harm cannot satisfy the requirement of concreteness," thereby providing a crucial caveat for BIPA plaintiffs.

Whether a person suffers real-world harm for a technical violation of BIPA remains unclear as federal courts come down on different sides of the issue. For example, in *McGinnis v. United States Cold Storage, Inc.*, an employee sued his employer for BIPA violations relating to the use of his fingerprints. The Illinois district court found the failure to provide and obtain BIPA's required notice or consent, without more, did not amount to a concrete

Photo Illustration: Elmarie C. Jara © Getty Images

injury. The court dismissed the case for lack of standing.

But in *Patel v. Facebook, Inc.*, a California district court found a statutory violation *did* amount to concrete harm. The plaintiffs claimed the defendant violated BIPA by failing to inform them that the "Tag Suggestions" program collected and stored their facial geometry. The court held these allegations were sufficient to confer standing, reasoning that "[a] violation of the BIPA notice and consent procedures infringes the very privacy rights the Illinois legislature sought to protect by enacting BIPA. That is quintessentially an intangible harm that constitutes a concrete injury in fact."

While *Rosenbach* is not authoritative, the opinion certainly lends support for those arguing in favor of Article III standing, agree Section leaders.

A Patchwork of Privacy Laws

Enacted in 2008, "BIPA was the first statute of its kind in the country and remains the strictest and, to my knowledge, the only one that includes a private cause of action," observes Vandesteeg. Two other states, Texas and Washington, have also enacted specific biometric privacy laws. Unlike Illinois, however, these states do not provide a private right of action. Nor do Texas and Washington require a particular form of notice or consent as BIPA does. BIPA also goes further than its state counterparts by requiring companies to develop and make public a written policy on biometric data retention and destruction.

Though BIPA is the harbinger, Section leaders note several other states are at varying stages of passing laws to protect biometric data, including Alaska, Arizona, Connecticut, Florida, Massachusetts, Montana, and New York. Each state's approach differs substantively. Some states grant private causes of actions, while others leave it to the attorneys general to enforce. States also differ on the required type of damages (i.e., actual or technical) to seek redress under the law. Even the definition of biometric information changes depending on the jurisdiction.

Beyond the biometric-specific laws, general consumer protection laws may extend protection to biometric information as well, say Section leaders. For example, "other states protect biometric privacy information through consumer protection laws, like the California Consumer Privacy Act, which allows a private right of action but only if the breach results in unauthorized use," contrasts Bilus. With these varying degrees of requirements among the states, "we are likely to see that if we don't have a broader federal policy, we will end up with a patchwork of biometric policy laws making it more difficult to comply and increase costs of how to handle information under this patchwork," opines Vandesteeg.

"Advising clients on biometric information is a combination of ensuring strict compliance with the provisions of the applicable law and being smart about having best practices in place for information security policies that are reasonably tailored to their business risks and needs."

Advice for Navigating the Privacy Matrix

So what steps *can* companies take to comply with existing laws and prepare for potentially applicable laws in the pipeline? "First, clients have to get an understanding of what personal information, including but not limited to biometric information, their company is collecting and using, and what current data-collecting and retention practices are," advises Bilus. "Is the company collecting biometric information? If so, is it meeting the notice and consent requirements? Is the company keeping adequate records to prove compliance in the event a BIPA-type lawsuit is filed? Look at third-party vendors that have access to the data and ensure the contracts with vendors have right provisions for using, disclosing, and protecting the data, along with an indemnification provision," Bilus counsels.

Companies can adopt best practices developed for handling their other electronic data, though some nuances exist given the particular sensitivity of biometric information. "Advising clients on biometric information is a combination of ensuring strict compliance with the provisions of the applicable law and being smart about having best practices in place for information security policies that are reasonably tailored to their business risks and needs," opines Vandesteeg. "In terms of mapping out your data, you need to know what divisions are collecting and using the biometric information and for what purposes," states Vandesteeg. "Then you can incorporate your biometric data into a broader institutional informational security program that includes training employees on proper use and destruction," Vandesteeg concludes. Above all else, "treat biometric information as your company's crown jewels," emphasizes Bilus.

RESOURCES

- Geoffrey J. Derrick, "The Forthcoming Wave of Biometrics Class Actions," *Consumer Litig.* (Mar. 19, 2019).
- *Rosenbach v. Six Flags Entertainment Corp.*, 2019 IL 123186 (Jan. 25, 2019).
- *McGinnis v. United States Cold Storage, Inc.*, No. 17 C 08054 (Jan. 3, 2019).
- *Patel v. Facebook, Inc.*, 290 F. Supp. 3d 948 (Feb. 26, 2018).
- Texas Business and Commerce Code § 503.001, Capture or Use of Biometric Identifier.
- Washington State Legislature, RCW 19.375.010.