New York Law Journal

NEW YORK LAW JOURNAL SPECIAL REPORT

ALM.

WWW.NYLJ.COM

MAY 20, 2022

Insurance Law

While New Biometric Privacy Laws Have Led to Widespread Litigation and Large Settlements, Most Courts Have Held That Insurance Covers These Claims

BY CORT T. MALONE AND JADE W. SOBH

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. Businesses use BII for various purposes including time cards, security, access to buildings or technology, or even for biometric marketing. 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. With the added convenience comes added risk, however, because your BII cannot be replaced or changed if stolen. The increased use of BII has predictably led to state regulation to protect consumers' and employees' biometric data.

Across the United States, legislatures are passing new biometric privacy laws with potentially onerous fines, making businesses who collect biometric information, and the insurance companies that sell policies to those companies, understandably nervous. These laws have varying impact depending on whether or not they create a private cause of action, how much the fines are per violation, and other provisions, such as the presence of a notice period and opportunity to cure.

Photo: Metamorworks via Adobe Stock

The Illinois Biometric Information Privacy Act (BIPA), enacted in 2008, was one of the first state laws to address business's collection of biometric data, and has resulted in some of the most notable lawsuits and settlements arising out of violations. BIPA requires companies to provide informed consent prior to collection, permits a limited right to disclosure, mandates protection obligations and retention guidelines, and prohibits profiting from biometric data. Most importantly from a liability standpoint, BIPA creates a private right of action for individuals subjected to BIPA violations, and provides statutory damages of at least $1,000 for each negligent violation and at least $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. Under the seminal decision in *Rosenbach v. Six Flags Entertainment*, 129 N.E.3d 1197 (Ill. 2019), 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 arguably has standing to sue under the Act. In so ruling, the Illinois Supreme Court reversed the appellate court's holding that Ms. Rosenbach and her son could not sue because they had suffered only a "technical violation" of the statute that did not cause any "actual injury." Understanding that the intention of the legislature was to pass a law that purposely made it easy for consumers to sue companies that violated their rights, the Illinois Supreme Court unanimously ruled in favor of Rosenbach, allowing her case to proceed, and protecting the effectiveness of BIPA for consumers.

Recently, an Illinois court approved a class action settlement of $36 million in this case, on behalf of individuals who had their fingerprints scanned at Six Flags amusement parks. BIPA has resulted in the largest settlements under biometric privacy laws and surely will continue to produce large class-action cases and sizable settlements.

The extensive liability arising out of BIPA has given rise to insurance coverage disputes. One of the first and most influential cases is *West Bend Mutual Insurance Co. v. Krishna Schaumburg Tan*, 166 N.E.3d 818 (Ill. App. Ct. 2020), aff'd, 183 N.E.3d 47 (Ill. 2021). Krishna Schaumburg Tan sought coverage for liability arising from regarding an underlying BIPA lawsuit under its Commercial General Liability (CGL) policy. The insurance company sought a declaration that it had no duty to defend or indemnify Krishna, arguing that the allegations did not fall within the type of injuries covered in the policy, and that even if the allegations did fall within the policy, a "violation of statutes" exclusion barred coverage.

The policy stated that the insurance company would pay "those sums that [Krishna] becomes legally obligated to pay as damages" because of personal injury arising out of oral or written publication of material that violates a person's right of privacy. The insurance company argued that the definition of publication did not encompass BIPA, but the court found that while "publication" meant "the broad sharing of information to multiple recipients," it also included "a more limited sharing of information with a single third party." Using the latter definition, the court found that by providing customers' fingerprints to a single third party, Krishna engaged in publication, an act covered by the insurance policies. The court also found that the "violation of statutes" exclusion did not apply to BIPA, as it differed from the other statutes enumerated in the exclusion. Accordingly, the court held that the insurance company had a duty to defend Krishna against the underlying BIPA complaint.

Earlier this year, one Northern District of Illinois trial court held that an "employment related practices" exclusion precluded a defense of BIPA claims brought by the policyholder's employees. The court in *American Family Mutual Insurance Co. v. Caremel*, No. 20-c-637, 2022 WL 79868 (N.D. Ill. Jan. 7, 2022) found that employees sharing their fingerprint data with their employer was part of their employment and therefore triggered the policy's Employment Related Practices exclusion. The policyholder did not appeal the trial court's decision.

All other recent BIPA coverage decisions in Illinois have been in favor of the policyholder. In *Twin City Fire Insurance Co. v. Vonachen Services*, No. 20-cv-1150-JES-JEH, 2021 WL 4876943 (C.D. Ill. Oct. 19, 2021), the Northern District of Illinois addressed coverage for two class actions arising under BIPA. Vonachen was sued for its use, collection, and storage of employees' fingerprints without consent. Vonachen was insured under a liability policy containing an Employment Practices Liability (EPL) coverage section, which defined a wrongful act as including any breach of a contract or employee manual. The court sided with Vonachen in holding that the policy's coverage language specifically applied where the company handbook required employees to use a biometric timekeeping system and simultaneously required the company to "comply with all applicable laws and regulations." The court granted Vonachen's motion for summary judgment and found that Twin City had the duty to defend Vonachen, thus demonstrating that there can be coverage for BIPA claims under EPL policies in addition to CGL policies.

Three other Illinois decisions—all from March of 2022—held in favor of coverage for BIPA violations despite insurance companies' efforts to apply exclusions to avoid liability for such claims. The first case, *Citizens Insurance Co. of America v. Thermoflex Waukegan*, No. 20-cv-05980, 2022 WL 602534 (N.D. Ill. March 1, 2022), stemmed from Thermoflex's assertion that its insurance companies were obligated to defend Thermoflex in a class-action lawsuit alleging that Thermoflex violated BIPA. After denying coverage, the insurance companies filed suit against Thermoflex, seeking a declaratory judgment confirming their denial.

Thermoflex's commercial lines policy provided coverage for "personal and advertising injuries," which included injuries arising out of "oral or written publication, in any matter, of material that violates a person's right of privacy." Because the issue involved the insurance companies' duty to defend, Thermoflex only needed to show that the underlying litigation was potentially or arguably within the scope of coverage. Significantly, on cross-motions for judgment on the pleadings, the court denied the insurance companies' motion, which asserted three separate exclusions applied to bar coverage: (1) an employment related practices exclusion; (2) a recording and distribution exclusion; and (3) an access

or disclosure exclusion, and granted judgment on the pleadings on behalf of Thermoflex. While Illinois courts have rejected application of these exclusions, one North Carolina court has applied a broader "recording and distribution" exclusion to deny coverage. In *Massachusetts Bay Insurance Co. v. Impact Fulfillment Services*, No. 20-cv-926-WLO, 2021 WL 4392061 (M.D.N.C. Sept. 24, 2021), the court held, under North Carolina law, that the newer wording of the "Recording and Distribution of Material or Information" exclusion was broader than the exclusion in *Krishna* and thus barred coverage.

In the second March 2022 Illinois decision finding coverage for BIPA liability, *State Automobile Mutual Insurance Co. v. Tony's Finer Foods Enterprises*, No. 1:20-cv-06199, 2022 WL 683688 (N.D. Ill. March 8, 2022), the court held that an insurance company must cover a grocery store in spite of an "employment practices" exclusion. The court found that the exclusion included a "laundry list" of targeted actions such as coercion, demotion, evaluation and discipline, but "[u]sing one's finger to clock-in and clock-out is an awkward fit in that string, at best." The court explained that, unlike the other items listed, clocking in with fingerprints did not affect an employee's standing with the company and was not related to mistreatment of a specific employee.

Finally, the Northern District of Illinois recently held that an IT services firm, Wynndalco Enterprises, was entitled to coverage on two potential class actions asserting that Wynndalco violated BIPA. *Citizens Ins. Co. of Am. v. Wynndalco Enters.*, No. 20-cv-3873, 2022 WL 952534 (N.D. Ill. March 30, 2022). Wynndalco allegedly profited from the acts of another company, Clearview AI, that allegedly had been "scraping" images and identifying information from Facebook, Twitter, Instagram, LinkedIn, YouTube, and other sites to create a database of facial scans. Wynndalco had no role in creating Clearview's products, but allegedly violated BIPA by purchasing licenses to use the product and then reselling those licenses at a profit. The court found that a "distribution of material in violation of statutes" exclusion was too broad, and did not clearly exclude claims of BIPA violations. While the policy purported to exclude coverage for alleged violations of statutes similar to the Telephone Consumer Protection Act, the CAN-SPAM Act, the Fair Credit Reporting Act, and the Fair and Accurate Credit Transaction Act, the court found that BIPA was categorically different. The court specifically found that the only resemblance between BIPA and the enumerated statutes is that they all protect privacy, but held that privacy under BIPA means something different than under those other statutes.

While BIPA is the most consumer friendly biometric privacy law, other states and municipalities also have passed laws to protect BII. In New York City, a biometric privacy law went into effect in July 2021 (NYC Admin. Code §§22-1201-1205), which also creates a private right of action, but includes a 30-day notice and cure period for commercial establishments. The notice-and-cure provision in the NYC law is likely preventing the onslaught of class-action lawsuits seen in Illinois. However, the New York state legislature is considering a bill to enact a law similar to BIPA that may include a similar private right of action. Other states, such as Washington and California, have passed biometric privacy laws that do not contain a private right of action, but rather are enforced by the state's attorney general. Many other states across the nation are considering bills on biometric privacy.

As companies learn how to adapt to these new laws, there will continue to be huge settlements in BIPA cases and high-stakes lawsuits in states where the Attorney General enforces biometric privacy laws. For example, in Texas, the Attorney General recently announced that Meta, Facebook's parent company, could be liable for billions of dollars' worth of damages under the state's Capture or Use of Biometric Identifier Act (CUBI). The Texas AG's announcement came after Facebook's own recent $650 million settlement for BIPA claims.

More state biometric privacy laws being passed means there will be more risks for companies using BII. And more BII liability risk means more insurance coverage disputes are sure to follow. Companies at risk of liability under biometric privacy laws need to scrutinize their existing liability coverage and be wary of insurance companies making changes to policy language or adding exclusions to coverage targeting biometric privacy claims when purchasing and renewing their insurance policies.

Cort T. Malone *is a shareholder at Anderson Kill P.C. He is chair of the firm's biometric liability group and a member of its insurance recovery group.* **Jade W. Sobh** *is an attorney at the firm and a member of its biometric liability and insurance recovery groups.*