

TOP STORY

Beware BIPA: Biometric Privacy Act Has Bite

By Grant H. Hackley – September 11, 2020

A business is entitled to insurance coverage for claims arising from violations of the Illinois Biometric Information Privacy Act (BIPA), even though the policy of insurance excluded coverage for violations of statutes, according to the [Illinois Court of Appeals, First District](#). In [West Bend Mutual Insurance Company v. Krishna Schaumburg Tan, Inc.](#), the court affirmed summary judgment in favor of an insured seeking coverage for a proposed class suit asserting technical breaches of privacy protections. However, experts suggest that the playing field is changing for biometric information breach claims, that insurance coverage is case specific, and that the bottom-line result is highly dependent upon jurisdiction.

Illinois Leads the Way

From the first successful criminal fingerprint identification in 1892, in Buenos Aires, Argentina, to the [first criminal trial in the U.S.](#) utilizing fingerprints for identification, held in Chicago in 1910, biometric fingerprint information has been collected and used for identification purposes. More recently, retinal scans, voice prints, and other identifiers have been perfected as a means of authenticating identity. With digital devices readily accessible to the average consumer, biometric information is easier than ever to collect and utilize. Global consulting firm [IHS Markit](#) predicted that, as of 2020, 1.6 billion mobile devices would come equipped with fingerprint scanners. However, [ABA Section of Litigation](#) leaders point out that only a handful of states have enacted regulations governing the use of biometric information, and that Illinois leads the way when it comes to policing privacy violations.

In 2008, Illinois enacted BIPA to grant consumer privacy protections for collected biometric information. Among the protections afforded is a requirement that written consent be obtained before information is shared with outside parties. The law was cited sparingly, until a 2019 decision by the [Illinois Supreme Court, *Rosenbach v. Six Flags*](#), held that a simple technical violation of the law is sufficient to impose the statutory penalties.

“*Rosenbach* opened the floodgates,” muses [Angela R. Elbert](#), Chicago, IL, former cochair of the Section of Litigation’s [Insurance Coverage Committee](#). After that holding, technical infringement of the statute was enough that “no proof of actual injury or damages was necessary to state a claim for a private cause of action,” explains Elbert, who also says that the Illinois statute is an outlier. The result is “a cottage industry for plaintiffs’ lawyers,” she adds. The ensuing deluge of litigation has caused a costly tug of war.

The Dam Bursts

In the *West Bend* case, Klaudia Sekura brought a putative class action against Krishna Schaumburg Tan, a franchisee of a tanning salon, for a technical BIPA violation. The underlying claim involved Ms. Sekura's assertion that when she registered for membership, Krishna collected her fingerprint for use as a biometric key to allow her access to the facility. Krishna shared the biometric information, the fingerprint, with a third-party vendor without first gaining Sekura's written consent.

West Bend, Krishna's insurer, defended Krishna under a reservation of rights and brought a declaratory action seeking to deny coverage. The trial court granted summary judgment in Krishna's favor, and the Appellate Court of Illinois, First District, affirmed. On appeal, West Bend argued that the BIPA violation did not constitute a personal injury under the policy and also that the policy's exclusion for violations of statutes governing communications barred coverage.

The court held that the sharing of data constituted a publication and could therefore be considered a personal injury, discussing the definition of the word "publication" in the context of both defamation and privacy claims. The court further reasoned that the policy's violations-of-statutes exclusion related to the means in which the information was shared, not the BIPA data-sharing violation itself.

West Bend has appealed, but Section leaders believe the decision was correct. "The exclusion in the West Bend policy was very narrow," notes Elbert. "Newer policy exclusions specifically refer to violations of BIPA, and I expect that to be the standard in the coming year," she predicts. She also adds that "once carriers pick up a claim, they will add this exclusion for the next policy year."

Jurisdictional Differences

"Illinois is alone among states with a private cause of action for a technical violation," observes [Grace C. Wen](#), Boston, MA, member of the Section's [Privacy & Data Security Committee](#) who presented on data privacy and BIPA at the 2020 Section Annual Conference. Other states, such as [Arkansas](#), California, [New York](#), [Texas](#), and [Washington](#), currently regulate the disclosure of biometric information, but the goal is remedial rather than remunerative. For example, in California, the recently enacted California Consumer Privacy Act ([CCPA](#)) requires exhaustion of other remedies before bringing litigation. "The CCPA focuses more on gaining consumer consent, confirming the information is correct, and having it deleted if you want," clarifies Wen.

By contrast, BIPA has teeth. Hefty penalties for technical violations—\$1,000 for a negligent violation and \$5,000 for a reckless or intentional violation—were probably a driving force behind Facebook’s \$550 million settlement of class claims for alleged facial recognition privacy violations. “Facebook didn’t have much of a defense,” opines Wen. “All the class had to do was show a technical violation.”

As a result, companies should be aware of the risk and determine whether they have coverage. “Businesses should take data privacy seriously,” advises Wen. “With more personal information available, it is more likely that a private company is going to be subject to litigation for disclosure of the data.”

And be dogged in seeking coverage, counsels Elbert. “Every litigator should look for insurance coverage when their client is sued for BIPA and CCPA violations. Don’t take no for an answer.”

[Grant H. Hackley](#) is a contributing editor for Litigation News.

Hashtags: #dataprivacy, #insurancecoverage, #biometrics

Related Resources

- Pamela Hans, John Lacey, & Marc Schein, “[Maximizing Coverage amid the Biometric Liability Wave](#),” *Insurance Coverage* (May 19, 2020).
- David Y. Loh, “[BNSF Subject to Class Action Based on Illinois Biometric Privacy Act](#),” *Admiralty Litig.* (Nov. 6, 2019).
- Brittany Levine, “[Privacy Settings May Not Protect Your Privacy from Facebook](#),” *Trial Practice* (May 30, 2018).