Biometric Information Privacy: Scanning the Coverage Issues

By Thomas W. Arvanitis and Haley E. Jauregui


What was once considered a concept of science fiction is now used by companies throughout the world on a daily basis. Much has been reported in the news on the uses and misuses of "biometrics." Generally, biometrics involves the measurement of a person's biological features. A fingerprint, an eye retina, and even a person's facial geometry are examples of the types of physical characteristics that biometrics can assess and measure.

The use of biometrics in the workplace is becoming more common. Some companies use biometrics to authenticate individuals before providing them access to secure or protected information or databases. Others use biometrics to catalog customers and track an employee's on-the-job comings and goings.

The enactment of privacy protection laws to address related privacy concerns means new liabilities. While these laws are now in a handful of states including Illinois, Washington, Texas, New York, and Arkansas, at the forefront is Illinois, which, a decade ago, was the first—and currently remains the only state—to create a private right action for such alleged privacy infringements.

Overview of State Biometric Privacy Statutes

Given biometric data's unique and personal nature, privacy is a significant concern. Not surprisingly, a handful of states have now enacted legislation to address how an entity stores and uses an individual's biometric data. For example, Washington prohibits an entity from "enrolling" a biometric identifier without providing notice, obtaining consent, or providing a mechanism to prevent subsequent use of the data for "commercial purpose." WASH. CODE. ANN. §19.375.020. Similarly, Texas's Capture or Use of Biometric Identifier Act (CUBI) outlaws the selling, leasing, use, and disclosure of biometric data without the owner's consent. TEX. BUS. AND COMMERCE CODE ANN. §503.001. CUBI requires that entities take "reasonable care" in storing biometric data and gives such entities a "reasonable [amount of] time" to destroy the data. *Id*. CUBI permits the state attorney general to seek $25,000 in civil penalties from those entities that violate CUBI. *Id.*

In New York, limited biometric legislation has precluded employers from non-voluntary fingerprinting of employees, unless otherwise authorized by law. *See* N.Y. Lab. Law §201-a. However, New York has now also amended existing data-breach notification laws with its "SHIELD" legislation—the Stop Hacks and Improve Electronic Data Security Act, which became effective in 2020. *See also* Ark. Code Ann. §4-110-101 (Arkansas Personal Information Protection Act).

California has now joined the mix as well, with the California Consumer Protection Act of 2018 (CCPA) going into effect on January 1, 2020. The CCPA grants certain rights to consumers with regard to the collection and use of their personal information, including biometric data. For example, qualifying businesses will be required to notify consumers of the collection of biometric data, how such data may be used, and the consumers' right to have the data deleted or to prohibit its sale to third parties.

Biometric privacy enactments in Washington, Texas, New York and Arkansas do not permit the owner of biometric data to bring a private right of action against an entity for its misuse of

biometric data. Nor does the CCPA. That is where Illinois's Biometric Information Privacy Act (BIPA) is different. BIPA is the only state biometric privacy statute that currently permits an owner of biometric data to bring a private right of action.

Consumer and Employee BIPA Litigation

BIPA prohibits an entity from collecting, capturing, purchasing, or receiving through trade a person's "biometric identifier" or "biometric information" unless that person receives written notice and gives consent to the collection, storage, use and disclosure of that data. 740 ILCS 14/1-30. BIPA also requires that an entity take reasonable care to safeguard the biometric data and limits retention of data to only the purpose for which it was collected. *Id.* Private entities are required to develop a publicly available written policy detailing their procedures for the retention and deletion of biometric data. *Id.* Any person "aggrieved" by a violation of the statute is not only entitled to her/his reasonable attorney's fees, costs, and injunctive relief, if appropriate, s/he may also seek $1,000 in liquidated dam-ages for an entity's negligent violation of BIPA, or $5,000 in liquidated damages for an intentional or reckless violation. *Id.* Significantly, the Illinois Supreme Court has held that a plaintiff need not sustain actual damage to establish that s/he is "aggrieved" under BIPA. *Rosenbach v. Six Flags Entm't Corp.*, 129 N.E.3d 1197 (Ill. 2019).

Since *Rosenbach*, courts have seen an increase in BIPA-related class action litigation. Although defendants have raised a number of defenses to BIPA claims, few have resulted in an outright dismissal of such claims. In August 2019, the Ninth Circuit Court of Appeals held that Facebook users had Article III standing to assert BIPA claims against the social networking giant, finding that BIPA protects an individual's concrete privacy interests, not mere procedural rights. *Patel v. Facebook*, 932 F.3d 1264 (9th Cir. 2019). Defendants' contentions that BIPA is preempted by various state and federal laws have also proven unsuccessful. *See, e.g., Rogers v. BNSF Railway Co*., No. 19-cv-3083, 2019 WL 5635180, at *4-5 (N.D. Ill. Oct. 31, 2019) (rejecting railway's argument that BIPA is preempted by federal laws regulating rail or ground transportation*); McDonald v. Symphony Bronzeville Park LLC*, No. 2017-CH-11311 (Cir. Ct. Cook Cnty. Ill. June 17, 2019) (rejecting defendant's contention that employee's BIPA claim was preempted by the Illinois Workers' Compensation Act).

Due to the general lack of successful defensive arguments, some litigants have opted to settle their BIPA disputes. While settlement amounts vary greatly, depending on the size of the class and the merits of the claim, BIPA claims have been settled for as much as $1,300 per class member. *Lloyd v. Xanitos, Inc.,* Case No. 2018-CH-1535 (Cir. Ct. Cook Cnty. Ill.).

Coverage Issues for BIPA Claims in Commercial General Liability Policies

With the rise of BIPA claims and the potential for substantial class action judgments or settlements, insurers are likely to see more and more requests for coverage under their liability insurance policies. While BIPA claims should not implicate a general liability policy's "bodily injury" or "property damage" coverages, the privacy interests at the heart of BIPA claims present novel "personal and advertising injury" coverage issues.

In standard Commercial General Liability policies, the term "personal and advertising injury" is typically defined as injury arising out of certain enumerated offenses, including the oral or written publication of material that violates a person's right of privacy. Through BIPA, the Illinois legislature "codified that individuals possess a right of privacy in and control over their biometric identifiers and biometric information." *Rosenbach*, 129 N.E.3d at 1206. A violation of one's privacy rights alone, however,

is insufficient to trigger coverage. Under the right of privacy offense, an insured must face liability for a publication—or a distribution to a third party—of material that violates a person's right of privacy. An insured's collection or recording of biometric data in violation of BIPA, in and of itself, does not involve a distribution of material to a third party. However, if an insured also faces BIPA claims predicated on the sharing of the plaintiff's biometric data with a third-party, the publication requirement may be satisfied. *See West Bend Mut. Ins. Co. v. Krishna Schaumburg Tan,* No. 2016 CH 7994 (Cir. Ct. Cook Cnty. Ill. May 14, 2018) (appeal pending) (finding allegations that insured disclosed claimant's fingerprints to a third-party vendor without the claimant's consent in violation of BIPA under the right of privacy offense).

Even if an insured's violation of BIPA triggers coverage under the right of privacy offense, however, there are at least two exclusions that may limit or preclude coverage.

First, ISO's 2013 CGL coverage form (CG 00 01 04 13) contains an Exclusion q. which bars coverage in connection with the "Recording And Distribution Of Material Or Information In Violation Of Law." In addition to excluding coverage for alleged violations of the TCPA, CAN-SPAM, FRCA and FACTA, this exclusion also precludes coverage for "personal and advertising injury" arising directly or indirectly out of any action or omission that violates or is alleged to violate any federal, state or local statute, ordinance or regulation that addresses, prohibits, or limits the printing, dissemination, disposal, collecting, recording, sending, transmitting, communicating or distribution of material or information. In *Rosenbach*, the Illinois Supreme Court recognized that BIPA places obligations on the collection of biometric identifiers and biometric information. 129 N.E.3d at 1203. Therefore, BIPA should qualify as a statute that addresses or limits the collecting and recording of material or information under the violation of law exclusion.

Whether courts will find the violation of law exclusion precludes coverage for BIPA claims, however, remains to be seen. In *Krishna Schaumburg Tan, supra*, the trial court found a similar exclusion added by endorsement did not preclude a duty to defend the BIPA claims against the insured. No. 2016 CH 7994 at *19–*21. However, the exclusion in that case was arguably narrower than the violation of law exclusion in more recent ISO forms in several key respects. For example, the exclusion at issue in *Krishna Schaumburg Tan* applied only to a statute that "prohibits or limits" the "sending, transmitting, communicating or distribution of material or information." The trial court found that BIPA is primarily concerned with regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric information, as opposed to its sending, transmission or communication. *Id.* at 19–20. The violation of statues exclusion in recent ISO forms applies to a statute that not only "prohibits or limits," but "addresses" the "collecting" and "recording" of material or information. As detailed above, BIPA addresses the collecting and recording of biometric information.

A second exclusion that may limit an insurer's obligations with respect to BIPA claims was introduced by ISO via a 2014 endorsement titled "Exclusion – Access or Disclosure of Confidential Or Personal Information and Data Related Liability – With Limited Bodily Injury Exception" (CG 21 06 05 14). This exclusion precludes coverage for "personal and 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. Biometric data protected under BIPA, including fingerprints, voiceprints, and hand or face geometry, are used to identify a person and by their very nature constitute personal information. The sharing or distribution

of biometric information under BIPA therefore constitutes the "disclosure of any person's . . . confidential or personal information." Again, however, application of the exclusion to BIPA claims remains untested in the courts.

In Conclusion

As BIPA cases and settlements continue, insurers can expect insureds to look to their liability policies as a source of defense and indemnity; but that does not mean the insureds are looking in the right place. Given the potential exposure BIPA claims can pose, insurers must be mindful of how courts are construing coverage in the context of these twenty-first century claims.

Moreover, given the trends toward the use of biometric data and legislation to protect related privacy rights, companies must be diligent in complying with the disparate state laws and keep abreast of legislation throughout the country. It may only be a matter of time before additional laws pop up affording the broad protections and a private right of action such as that found in BIPA.

Thomas W. Arvanitis is a partner of Nicolaides Fink Thorpe Michaelides Sullivan LLP in Chicago. Tom provides coverage advice and represents insurers in complex litigation involving declaratory relief, extra-contractual claims, and appeals. Tom has significant experience advising insurers with respect to personal and advertising injury coverage, including intellectual property claims, privacy claims, and unfair business practice claims. Tom also has experience in analyzing pollution liability, construction, and product defect claims under various lines of coverage.

Haley E. Jauregui is an associate in the Chicago office of Nicolaides Fink Thorp Michaelides Sullivan LLP, where she focuses on insurance coverage analysis and litigation. Her practice includes assessing and evaluating construction defect, environmental, and primary and excess general liability-related coverage issues.