FEDERATION OF REGULATORY COUNSEL

The Illinois Biometric Information Privacy Act: Emerging Insurance Issues

Daniel A. Cotter, Esq.
Howard & Howard Attorneys PLLC
(312) 456-3674 | dcotter@howardandhoward.com

In 2008, the Illinois legislature passed the Illinois Biometric Information Protection Act ("BIPA").[1] The act regulates the "collection, use, safeguarding, handling, storage, retention and destruction of biometric identifiers and information."[2] The law for many years was dormant, with only 15 class actions being filed in its first nine years.[3] But then savvy plaintiffs lawyers found that this statutory penalties legislation provided a potential treasure trove of recoveries, and in the next few years, the number of class actions hitting 161 in 2019.[4] With the burgeoning arena of BIPA class actions, defendant employers and service providers have sought insurance coverage. This article addresses some of the insurance issues that have arisen and likely will arise.

What BIPA covers

The definition of biometric identifier includes "a retina or iris scan, fingerprint, voiceprint or scan of hand or face geometry."[5] The law was introduced and became law in response to various stores in Chicago, including Jewel Food Stores, setting up pilot programs in Chicago to test the evolving technology for point of sale fingerprint scanners.

The act provides for the awarding of statutory damages in amounts of the greater of $1,000 or actual damages for each negligent violation and $5,000 or actual damages for intentional violations, plus reasonable attorney fees, litigation expenses and costs.

Following the trend of class-action lawyers seeking statutory frameworks that provide for such statutory damages, many putative class actions were filed under the act beginning in 2016. In December 2016, the Courts in *Sekura v. L.A. Tan*.[6] approved the first settlement under the act.

Suits have been filed against Google, Facebook, Apple, and other platforms utilizing facial recognition software. In addition, several class actions have also been filed against employers alleging violations of the act for failure to disclose to employees the storage techniques and obtaining employee consent as required by the statute.

For example, a lawsuit was filed against Roundy's in May 2017[7], alleging that the supermarket chain requires employees to utilize a "biometric fingerprint time clock" when checking in and out of work.

Illinois is the only state that has enacted legislation addressing biometric information that provides a private right of action against alleged offenders. While Texas and Washington have legislation similar to Illinois' act, neither permits a private right of action — only the attorney general of each respective state may initiate action against alleged violators.

BIPA has several different ways in which holders of biometric information may violate BIPA.[8] The 7th Circuit has reviewed standing under subsections (a) through (c) of Section 15.

Six Flags and Standing

In 2019, the Illinois Supreme Court handed down its decision in *Rosenbach v. Six Flags Entm't Corp.*,[9] which held that "a person need not have sustained actual damage beyond violation of his or her rights under the Act in order to bring an action under it."[10] The court noted, "[t]hrough the Act, our General Assembly has codified that individuals possess a right to privacy in and control over their biometric identifiers and biometric information"[11] and that the "violation, in itself, is sufficient to support the individual's or customer's statutory cause of action."[12]

In August 2015, plaintiffs filed a putative class action in the United State District Court for the Northern District of California.[13] The complaint "alleges that Facebook subjected them to facial-recognition technology without complying with an Illinois statute intended to safeguard their privacy."[14] Facebook had created a new feature called "Tag Suggestions" that permits Facebook "to analyze whether the user's Facebook friends are in photos uploaded by that user."[15] The class consisted of "Facebook users living in Illinois"[16] who alleged violations of BIPA.[17] After analyzing BIPA, the Court noted "BIPA also provides for actual and liquidated damages for violations of the Act's requirements."[18]

Article III standing requires that a plaintiff "'have suffered an 'injury in fact'" that is "concrete"[19] but "need not be tangible."[20] The *Patel* panel discussed the *Robins v. Spokeo, Inc.* Supreme Court decision to address statutory provisions and actual harm suffered by those seeking damages.[21] It then considered the establishment of right to privacy actions.[22] After doing so, the court concluded "that an invasion of an individual's biometric privacy rights 'has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts.'"[23] The Court held: "Therefore, we conclude that 'the statutory provisions at issue' in BIPA were established to protect an individual's 'concrete interests' in privacy, not merely procedural rights."[24] Citing *Rosenbach*, the court that "the plaintiffs have alleged a concrete injury-in-fact sufficient to confer Article III standing."[25] Finally, with respect to the certification of the class, the court rejected Facebook's arguments about extraterritoriality, finding that "it is reasonable to infer that the General Assembly contemplated BIPA's application to individuals who are located in Illinois, even if some relevant activities occur outside the state."[26]

The 9th Circuit refused a petition for rehearing *en banc*, and the Supreme Court rejected the petition for certiorari.

The 7th Circuit, which includes Illinois, has reviewed standing issues as well. In *Christine Bryant v. Compass Group U.S.A., Inc.*,[27] the court held that the Complaint had satisfied the injury-in-fact requirement of Article III with respect to Plaintiff's claims under Section 15(b)[28] but did not satisfy the hurdle for Section 15(a).[29]

Workers Compensation Insurance Coverage

A recent Illinois appellate court decision investigated the issue of whether Workers' Compensation was the sole remedy for an employee who alleged violations of the Illinois BIPA. In *McDonald v Symphony Bronzeville Park LLC*,[30] the court held that the exclusive remedy of Workers' Compensation does not prohibit employees from bringing an action against an employer for allegedly violating the Illinois BIPA. While acknowledging that the Illinois Supreme Court "'has indicated that the [Compensation Act] generally provides the exclusive means by which an employee can recover against an employer for a work-related injury,'"[31] the court found that the exception for "not compensable" under the Workers' Compensation Act provided the out for the plaintiff in this case, holding:

> "In light of the above discussion, we fail to see how a claim by an employee against an employer for liquidated damages under the Privacy Act—available without any further compensable actual damages being alleged or sustained and designed in part to have a preventative and deterrent effect—represents the type of injury that categorically fits within the purview of the Compensation Act, which is a remedial statute designed to provide financial protection

> for workers that have sustained an actual injury. As such, we conclude that the exclusivity provisions of the Compensation Act do not bar a claim for statutory, liquidated damages, where an employer is alleged to have violated an employee's statutory privacy rights under the Privacy Act, as such a claim is simply not compensable under the Compensation Act."[32]

General Liability and Other Liability Policies

In *West Bend Mutual Ins. Co. v. Krishna Schaumburg Tan. Inc.*,[33] an Illinois appellate court in a case of first impression, the *Krishna* court affirmed the grant of summary judgment in favor of the insured and held that underlying complaint sufficiently alleged "publication" to trigger the duty to defend a BIPA claim and the exclusion for statutory violations that mentioned the TCPA and the Can-Spam Act, but not BIPA, did not apply. The appellate court also found:

> "In short, the violation of statutes exclusion applies to bar coverage to violations of statutes that regulate methods of communication. The Act says nothing about methods of communication. It instead regulates 'the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.' 740 ILCS 14/5(g)."[34]

The Illinois Supreme Court granted petition for leave to appeal and will hear oral arguments on the case some time in the coming months.

The arguments over whether liability policies cover BIPA center around whether any "personal injury" has occurred and given the nature of the damages as being statutory in nature, arguments continue about potential coverage.

In a recently filed case in Cook County, *American Guarantee & Liability Insurance Co. v. Toms King, LLC*, No. 2020-CH-04472 (Cir. Ct. Cook County June 5, 2020), the insurer argued that two arguing two exclusions allow it to provide no defense or coverage: employment-related practices and disclosure of confidential information.

Other Insurance Coverages

Many of the class action defendants are employers who have required their employees to use biometric information for signing in and out of their workday.[35] Many EPL policies contain exclusions for violations of statutes, but also might include invasion of privacy or failure to provide adequate corporate policies in the definition of "employment practices wrongful act," which may trigger coverage under the EPL policies.[36]

Another potential avenue of insurance coverage likely to be pursued is in the cyber arena. Today's entities are facing an evolving, wide-ranging specter of cyber and privacy risks that extend far beyond traditional notions of cyber security. As privacy laws and regulations continue to proliferate, the ways entities collect, use, store, share, and dispose of information can lead to legal and regulatory exposures, even in the absence of a data breach. Cyber insurance applicability will necessarily include a detailed analysis of how the policy defines covered information; and intentional conduct and statutory penalties might not be covered.

The insurance coverage determinations will vary by insurance type.[37] Policy language and type of policy will be important. As the Illinois courts see more insurance coverage disputes related to BIPA, the landscape should become more apparent.

Conclusion

With the *Six Flags* decision and other developments, plaintiffs likely will continue to aggressively seek relief from large defendants such as Facebook. For example, in November, a federal court in

Illinois rejected efforts by defendant Apple to dismiss a class action complaint filed against it.[38] The search for insurance coverage and money to pay for the continued substantial exposures defendants face continues. The availability of coverage under any policy will depend on the claim specific facts, the type of harms alleged, and policy terms and court applications of same and applicable law.

---

[1] The Biometric Information Privacy Act, 740 ILCS 14/1 *et seq.* (2008).
[2] 740 ILCS 14/5 (g).
[3] *See*, Seyfarth, Workplace Class Action Blog, "Biometric Privacy Class Actions By The Numbers: Analyzing Illinois' Hottest Class Action Trend," June 29, 2019, available at https://www.workplaceclassaction.com/2019/06/biometric-privacy-class-actions-by-the-numbers-analyzing-illinois-hottest-class-action-trend/.
[4] *Id.*
[5] 740 ILCS 14/10.
[6] Docket can be found at https://www.bloomberglaw.com/public/desktop/document/SEKURA_KLAUDIA_v_L_A_TAN_ENTERPRISES_INC_Docket_No_2015CH16694_Il?1481123411.
[7] *Norman Baron v. Roundy's Supermarkets Inc.*, 2017CH03821.
[8] 740 ILC 14/15. Section 15 provides:

> Sec. 15. Retention; collection; disclosure; destruction.
> (a) A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.
> (b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:
> (1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
> (2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
> (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.
> (c) No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information.
> (d) No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:
> (1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;
> (2) the disclosure or redisclosure completes a

financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative;

(3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or

(4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

(e) A private entity in possession of a biometric identifier or biometric information shall:

(1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and

(2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

[9] *Rosenbach v. Six Flags Entm't Corp.*, — N.E.3d —, 2019 IL 123186 (Ill. 2019), available at https://courts.illinois.gov/Opinions/SupremeCourt/2019/123186.pdf.
[10] *Id at* ¶ 28.
[11] *Id at* ¶ 33.
[12] *Id.*
[13] Original complaint available at https://epic.org/amicus/bipa/patel-v-facebook/Patel-v-FB-Consolidated-Class-Action-Complaint.pdf.
[14] *Patel,* p. 4.
[15] *Id* at 5.
[16] *Id* at 6.
[17] *Patel*, p. 6-7.
[18] *Id* at 9.
[19] *Id* at 10.
[20] *Patel,* p. 11.
[21] *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016), *as revised* (May 24, 2016), (*Spokeo I*) and *Robins v. Spokeo, Inc.*, 867 F.3d 1108, 1113 (9th Cir. 2017) (*Spokeo II)*.
[22] *Patel*, pgs. 13-16.
[23] *Id* at 16.
[24] *Id* at 18.
[25] *Patel*, p. 19.
[26] *Id* at 22.
[27] *Christine Bryant v. Compass Group U.S.A., Inc.*, No. 20-1443, 2020 WL 2121463 (7th Cir. 2020).
[28] *Id.*
[29] *Id.*
[30] *McDonald v Symphony Bronzeville Park LLC*, 2020 IL App (1st) 192398, ¶ 14 (2020) [2020 WL 5592607].
[31] *McDonald*, 2020 IL App 192398, ¶ 18.
[32] *Id at* ¶ *27.*
[33] *West Bend Mutual Ins. Co. v. Krishna Schaumburg Tan. Inc.*, 2020 IL App (1st) 191834.
[34] *Id.*
[35] In the current work from home environment, that might be less applicable, but many workers are still physically at their place of employment.
[36] *See, for example*, Berkley Insurance Company Employment Practices Liability Insurance, Section 2.E.(7), which defines employment practices wrongful act to include and mean:
"failure to provide or enforce adequate or consistent corporate policies and procedures relating to any **Employment Practices Wrongful Act**," available at http://www.berkleypro.com/wp-content/uploads/2018/12/PC_Policy_EPL_Coverage_Part.pdf.
[37] In a recent petition for certiorari that if granted would change the way policies of insurance are interpreted, the petitioner is asking the Supreme Court of the United States to make consistent how direct physical loss is interpreted among the federal circuit courts of appeals. *See Mama Jo's Inc. dba Berries v. Sparta Ins. Co.*, (11th Cir. 2020), available at https://cases.justia.com/federal/appellate-courts/ca11/18-12887/18-12887-2020-08-18.pdf?ts=1597755644.

[38] *See https://www.natlawreview.com/article/bipa-lawsuit-proceeds-against-apple-federal-court.*