2022 Focus December Conference
December 1, 2022
New York, New York

Facing the Issue: Coverage for Biometric litigation

Technology plays a vital role in the modernization of our society. We are fortunate that so many functions, which only a few years ago were more difficult and time consuming, have been streamlined. However, speed and efficiency have sometimes led to a loss of privacy, in particular with biometric data, which many consumers are not even aware of. People are using their own biometric data, such as fingerprints and retinal scans, in more ways than ever. From touchpads that unlock smartphones and computers, to scanners providing access to places of business, biometric data seems to be a fast, easy and secure way to authenticate someone's identity and grant access. That said, the collection and storage of biometric data can be a risky proposition for organizations that are not aware of the growing number of biometric data privacy laws. While the Illinois Biometric Privacy Act ("BIPA") is one of the more prevalent and oft-cited laws on this topic, there are many other state and local biometric privacy laws that are currently in place and more being considered. With this growing risk, many organizations are looking to take steps to understand the scope of their biometric collection and maintenance. They are also seeking insurance coverage that can help respond to such risks. As the use of biometric data continues to grow, the risks will follow and questions will remain as to what type of insurance coverage may help organizations minimize their exposure.

Privacy Laws

In general, compliance with federal, state and foreign privacy laws and regulations is now an essential obligation for both large and small businesses. These laws govern a company's collection, storage, use, sharing and disposal of personally identifiable information ("PII"), protected health information ("PHI") and payment card information ("PCI"). The laws protecting "biometric identifier information" – defined broadly to mean a "physiological or biological characteristic that is used by or on behalf of a commercial establishment, singly or in combination, to identify, or assist in identifying, an individual" – are similar in protecting how such data is used. Unlike PII, biometrics cannot be changed or altered if compromised. As such, the laws protecting such information are often strict. A company's inadvertent failure to abide by these laws, or its failure to timely and fully disclose how it performs such tasks, can make it a target for regulatory proceedings and civil class actions. These lapses also can be a source of reputational damage to the business. Notably, a significant number of public and private entities still remain unaware of the laws that govern consumers' and employees' privacy rights, as well as the risks and exposures.

BIPA

The most well-known and litigated state biometric law is Illinois' BIPA. While other states and municipalities have biometric protection laws, Illinois is the oldest (enacted in 2008) and one of the few that provides a private right of action for individuals to recover statutory damages based on an organization's failure to comply with the law. At its core, BIPA looks to protect the "biometric information" of Illinois residents, which is information based on "biometric identifiers" that identify a specific person – regardless of how it is captured, or shared. Biometric identifiers include retina or iris scans, fingerprints or palm prints, voice recognition, facial-geometry recognition, DNA recognition, gait recognition, (even) scent recognition. It does not include "writing samples," "written signatures," . . . "human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical characteristics such as height, weight, hair color, or eye color." Photographs are not considered biometric data, but the manner in which certain facial recognition mechanisms are applied to photos has been the source of litigation.

There are a couple of key sections under BIPA that other state and local laws protecting biometric data follow. First, Section 15(a) requires that a private entity have a written, publicly-available policy establishing collection, retention, storage and destruction guidelines for the biometric information it collects. Second, Section 15(b) requires that informed consent and a written release be executed ***before*** a private entity obtains a person's biometric identifier. Third, Section 15(c) states that no private entity may sell, lease, trade, or otherwise profit from a person's biometric identifier or biometric information. Fourth, Section 15(d) limits when a private entity can disclose a person's biometric information to a third party. Finally, Section 15(e) outlines the standard of care for the retention and storage of biometric information. The statutory penalties are $1,000 for each negligent violation and $5,000 for each intentional violation. Based upon the above, BIPA has quickly become a rising class action battleground – primarily due to the fact it allows a private right of action, statutory damages, and a low bar for establishing harm.

Other Biometric Privacy Laws

BIPA may be one of the most prominent biometric privacy laws, but it is far from the only one. In 2009, Texas passed its own act that imposes a steep $25,000 penalty for each violation. Importantly, however, it does not allow a private right of action. Only the state attorney general can bring an action to enforce the statute. Similar biometric laws were passed by Washington (2017), California (2020 – the Consumer Privacy Act), and Arkansas (2020), all of which do not allow a private right of action.

Local municipalities have also started addressing the issue of biometric privacy. For example, Portland (Oregon) prohibits the use of facial recognition technology by both government agencies and private businesses. This ordinance allows for a private right of action, and recoverable damages of $1,000 for each day of the violation. New York City's (New York) biometric privacy ordinance, which went into effect in July 2021, bans commercial establishments from selling or sharing customers' and employees' biometric information. It also requires commercial establishments to have clear signage about their policy. Similar to Portland, this local law does allow a private right of action, enabling aggrieved parties to collect statutory damages — ranging from $500 to $5,000 — per violation. These other states and municipalities, as well as the other jurisdictions with proposed legislation in the pipeline, reflect the growing emphasis on the protection of biometric data.

Significant Litigation

One of the reasons BIPA has become the most well-known biometric privacy law is the size and scope of litigation and settlement that has resulted under its "private right of action" provision. Despite numerous challenges, this provision has been upheld by a number of courts; particularly, in recent years.

The most significant of these rulings is *Rosenbach v. Six Flag Entm't Corp*., 2019 IL 123186 (Ill. 2019), where the Illinois Supreme Court held that a plaintiff can be an "aggrieved person" under the statute and "be entitled to liquidated damages and injunctive relief" without alleging an actual injury. This holding opened the proverbial floodgates. Before *Rosenbach*, many lawsuits alleging a BIPA violation were dismissed based upon decisions that held "a bare procedural violation, divorced from any concrete harm," fails to satisfy the injury-in-fact requirement to show "standing" to sue under Article III of the US Constitution. *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016). *Rosenbach* changed this for alleged BIPA violations when it found that BIPA did not require an actual injury; reasoning that when biometric information is involved, it is "no mere technicality" and "[t]he injury is real and significant." This decision dramatically increased the number of BIPA class actions. In 2018, there were only 79 filed. In just the first six months following *Rosenbach*, there were 151 filed.

Subsequently, other rulings have helped shape and clarify BIPA. In *Tims v. Black Horse Carriers, Inc.*, 184 N.E.3d 466 (Ill 1st Dept, 2021), the Illinois Appellate Court considered the limitation period governing BIPA claims; namely whether the one year limitations period for matters involving violation of privacy applied (735 ILCS 5/13-201) or the five-year "catch all" provision for "all civil actions not otherwise provided for" by statute applied (735 ILCS 5/13-205). Ultimately, the *Tims* Court held that the one-year limitations period applies to Sections 15(c) and (d) of BIPA, reasoning that these sections concern publication, and thus, implicate invasion of privacy concerns. As to the remaining sections (Sections 15(a), (b) and (e)), the court applied the five-year limitations period.

Another decision that has recently impacted the breadth of BIPA is *McDonald v. Symphony Bronzeville Park, LLC,* 2022 IL 126511 (IL Feb. 3, 2022), which held that the exclusivity provisions of the Illinois Workers' Compensation Act do not preempt employees' claims for damages against their employers under BIPA. The Illinois Supreme Court found that the statutory damages under BIPA are "not compensable" injuries, since they are neither psychological nor physical work injuries. As such, it held that the Illinois Workers' Compensation Act does not bar BIPA claims.

Notably, there have also been some defenses raised that have led to the dismissal of BIPA claims. One such argument relates to a company's enforcement of an arbitration agreement. In *Miracle-Pond v. Shutterfly, Inc*., 2020 US Dist Lexis 86083 (N.D. Ill. May 15, 2020), the court held that a plaintiff was required to pursue her BIPA claims in individual arbitration, despite the fact the arbitration provision was not added to the company's Terms of Use until a year after the plaintiff originally agreed to them. Another argument that has been raised, with some mixed success, is a challenge to personal jurisdiction where the activity at issue – *i.e*., the collection and storage of biometric information – took place in a state other than Illinois. In *McGoveran v. Amazon Web Services, Inc*., 488 F. Supp 3d 714 (S.D. Ill. Sept. 18, 2020), the court dismissed a lawsuit claiming Amazon Web Services, Inc. ("AWS") captured voice data based on phone calls placed in Illinois through its AWS' connect service, finding a lack of personal jurisdiction when the call center was located in Massachusetts and the only connection to Illinois was that Illinois citizens were being called. That said, recently, in *Crumpton v. Haemonetics Corp.*, 2022 U.S. Dist. LEXIS 58354, at *23-24 (N.D. Ill. Mar. 30, 2022), the court found that when a defendant in did have direct contact to Illinois, there was sufficient personal jurisdiction for a BIPA claim. These cases reflect that while standing arguments have largely been unsuccessful in defeating BIPA claims, lack of personal jurisdiction and enforcement of express arbitration agreements have found some success.

Ultimately, as the number of BIPA-related actions has grown since *Rosenbach*, the settlements have likewise increased, and in many instances, have been staggering. In 2020, Facebook settled its BIPA claim for $650 million. *Patel v. Facebook, Inc.* 2019 U.S. App. LEXIS 23673 (9th Cir. Aug. 8, 2019). In 2021, the *Rosenbach* case itself was settled for $36 million. In 2022, the settlements remain significant. In *Rivera, et al. v. Google LLC,* IL Cir Ct, Cook County, No. 2019-CH-00990, Google (tentatively) settled for

$100 million, with a final approval hearing set for late September 2022. In *Adrian Coss et al. v. Snap Inc*., No. 22-cv-02480 (N.D. Ill.), the parties reached a (tentative) settlement for $35 million. These cases reflect how significant and costly it can be when a business fails to comply with the regulatory framework of BIPA.

Coverage issues related to BIPA and potentially other statutes regarding biometric information

With a seemingly, ever-growing amount of litigation involving BIPA claims, there has likewise been a surge in litigation related to insurance coverage for such claims; namely, under commercial general liability ("CGL") policies. Not surprisingly, Illinois has a large amount of decisions in this regard; though other states have weighed in as well.

In *West Bend Mutual Ins. Co. v. Krishna Schaumburg Tan Inc.,* 2021 IL 125978 (Ill. 2021), the Illinois Supreme Court found that coverage was triggered under the "personal and advertising injury" insuring agreement of a CGL policy. It determined that (allegedly) providing fingerprinting data to third parties is a form of "publication" within the meaning of the policy. It also held that neither exclusions for "Violation of Statutes that Govern E-Mails, Fax Phone Calls or Other Methods of Sending Material or Information" nor a Telephone Consumer Protection Act ("TCPA") Exclusion precluded coverage. In rejecting these exclusions, the Court reasoned that TCPA exclusion did not apply to statutes like BIPA, but only as to statutes governing *methods* of communication. Various aspects of the decision in *West Bend* have been followed in such cases as: *Citizens Insurance Company of America et al. v. Thermoflex Waukegan LLC et al.*, 2022 US Dist Lexis 35630 (N.D. Ill. March 1, 2022), and *Am. Family Mut. v. Carnagio Enter.*, 2022 U.S. Dist. LEXIS 58358 (N.D. Ill. Mar. 30, 2022).

Separately, other courts have evaluated BIPA claims under separate exclusions, such as the employment practices exclusion. In this regard, Illinois courts have differed on whether coverage should be permitted. *See e.g*. *State Automobile Mutual Insurance Co. v. Tony's Finer Foods Enterprises Inc. et al*., 2022 US Dist Lexis 40567 (N.D. Ill. March 8, 2022) (BIPA not excluded by the employment practices exclusion); *but see*, *Church Mut. Ins. Co. v. Prairie Village Supporting Living, LLC*, (N.D. Ill. Aug. 11, 2022) (holding that "the Violations of Laws Applicable to Employers exclusion under the EPL coverage bars coverage" for the underlying lawsuit because "BIPA is categorically different than the enumerated exempted statutes"). Ultimately, the potential insurance coverage considerations and concerns are not going away, and a number of coverage disputes related to BIPA remain pending in Illinois courts; including *Am. Guarantee & Liab Ins Co. et al. v. Congress Plaza Hotel LLC et al.*, case no 22-CH-6870, Circuit Court of Cook County, IL.; *Citizens Ins. Co. v. Cooler Screens*, 22-cv-3800, US Dist, ND IL; and *Secura Insurance Co. v. Biometrics Impressions Corp.*, case number 2022-CH-08080, in the State of Illinois Circuit Court of Cook County. In sum, even under Illinois law, the overall potential for insurance coverage for BIPA claims remains unclear.

One other state where there are a number of coverage decisions involving BIPA and similar privacy statutes is North Carolina. In *Massachusetts Bay Insurance Company et al. v. Impact Fulfillment Services, LLC*, 2021 US Dist Lexis 182970 (M.D.N.C. Sept. 24, 2021), a federal court applying North Carolina law held the broader Recording and Distribution of Material or Information in Violation of Law Exclusion precluded a defense obligation for a BIPA claim because it excluded coverage for claims under statutes that protect and govern privacy interests in personal information. The court noted that "BIPA is of the same kind, character and nature as the listed statutes, this court finds that the Recording and Distribution of Material or Information Exclusion applies." Other North Carolina court have precluded coverage for privacy matters under the TCPA exclusions, such as with *AMCO Ins. Co. v. Van Laningham & Associates, PLLC*, 2022 US Dist Lexis 126956 (E.D. N.C. July 18, 2022) and *Main St. Am. Assurance Co. v. Crumley Roberts, LLP*, 2021 US Dist Lexis 60183 at *2 (M.D.N.C. Mar. 30, 2021). These North Carolina

cases, while they may be different than some of the cases in Illinois and each matter has different policy language, reflects the concerns on coverage for BIPA and other related biometric privacy matters.

The Next Battlegrounds and Where Things Go From Here

Issues regarding biometric privacy does not appear to be going away. Illinois may be on the forefront of protecting its citizen's biometric information, but it is not alone in that regard. There is a greater awareness of technology becoming more connected with our lives. Privacy legislation and litigation have been increasing in the past couple of years, and efforts to protect biometric privacy as increased in turn. As more and more states pass comprehensive privacy laws, companies that collect and use biometric data or plan to do so need to pay close attention to creating policies and procedures, implementing appropriate security measures, and being aware of the notice and consent requirements various laws impose. This is put a greater spotlight on issues of notice and consent with respect to collection of such information, as well as having a written retention and destruction policy. It has also led to greater awareness of security requirements for protecting such information, as well a restriction on disclosures. This includes understanding what insurance provides for coverage of such litigations. To minimize their risk, businesses must implement heightened awareness of the current and anticipated laws, be aware of the technical requirements, be vigilant with respect to compliance, and be aggressive in defending against litigation. Litigation surrounding biometric privacy appears to be only increasing, and as such understanding of the implications of protecting such information is only growing in importance.