Bloomberg Law®

Class Action Litigation Report®

Class Actions

Biometric Privacy Litigation: The Next Class Action Battleground

Litigation under the Illinois Biometric Information Privacy Act will continue to flourish until courts show a willingness to interpret BIPA narrowly and dismiss class actions at an early stage, attorneys Steven Grimes and Eric Shinabarger say. Any organization that collects or uses biometric data should closely examine its privacy practices for possible liability under the law, the authors say.

BY STEVEN GRIMES AND ERIC SHINABARGER

In the past year, the class action plaintiffs' bar has discovered a new statutory tool, complete with a large pool of potential plaintiffs, high statutory damages, and a private right of action: the Illinois Biometric Information Privacy Act (BIPA). 740 ILCS 14/1.

Although BIPA was enacted in 2008, litigation under the statute began in earnest in 2015, with several high-profile suits against social media websites alleging improper collection of facial geometries in photographs without notice and consent. *See, e.g.*, *Norberg v. Shutterfly, Inc.*, No. 1:15-cv-5351 (N.D. Ill.).

Since that time, over 60 class action complaints have been filed, vaulting BIPA into the spotlight alongside the Telephone Consumer Protection Act as one of the hottest class action trends. Notably, these claims are being brought against companies in various industries, targeting companies that use biometrics (usually fingerprints) to track the time worked by their employees in Illinois.

Winston & Strawn LLP partner Steven Grimes is a former federal prosecutor, an experienced trial lawyer, and a former Chief Compliance Officer and senior litigation counsel for a global publicly traded Fortune 500 company. Steve's practice focuses on compliance and data security counseling, sensitive internal investigations, and complex litigation.

Winston & Strawn LLP associate Eric Shinabarger focuses on patent and securities litigation, white collar defense, data breach response, and privacy consulting. Eric has represented several Big 4 accounting firms in enforcement actions brought by the Public Company Accounting Oversight Board.

BIPA litigation is spurred on by a private right of action that allows plaintiffs to seek $1,000 for each ''negligent'' violation of the act, and $5,000 for each ''intentional or reckless'' violation, plus attorneys' fees. 740 ILCS 14/20. While the scope of an ''intentional violation'' is untested, plaintiffs are seeking huge damages by, in some instances, claiming that each use of biometric information by an organization (*e.g.*, each swipe of a fingerprint to clock an employee in or out) constitutes a separate intentional violation of the law. While it is unclear at this stage whether the courts will accept the argument that each use of biometric information without notice constitutes a separate BIPA violation, these high statutory penalties raise the stakes and attract the plaintiffs' bar.

Summary of BIPA *Defining Biometric Information*

Generally, BIPA regulates, but does not forbid, the collection and storage of biometric identifiers. The law defines biometric identifiers as a ''retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.'' 740 ILCS 14/10. This definition affirmatively excludes other data points such as photographs, demographic data, and writing samples. *Id.* Similarly, the law also governs ''biometric information''—defined as ''any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual''—which is seemingly intended to prevent organizations from cir-

 ISSN 1529-0115

cumventing BIPA by converting biometric identifiers into other formats. This definition does not include information that is derived from biometric identifiers.

The Requirements of BIPA

Under BIPA, in order to collect or store biometrics, an employer must first: 1) provide written notice to individuals that the collection will occur as well as the purpose and length of the collection; and 2) receive informed written consent from the individual to proceed with the collection. Beyond the notice and consent requirements, BIPA also requires employers collecting or storing biometric identifiers to publish a privacy policy that details the organization's document retention policy for biometric data. BIPA also has a purpose-limitation component that requires organizations to destroy collected biometric data once the purpose for which it was collected ''has been satisfied'' or within three years of the organization's last interaction with the individual, whichever occurs first.

Importantly, before sharing biometric data with third parties, an employer must first obtain additional consent beyond the initial required consent. 740 ILCS 14/15(d)(1). Moreover, BIPA forbids organizations from ''selling'' or ''otherwise profiting from'' individuals' biometric information, although the contours of this vague restriction have not yet been defined by the courts. 740 ILCS 14/15(c).

Finally, BIPA requires that employers in possession of biometric information use the same data security precautions that they use for ''other confidential and sensitive information.'' 740 ILCS 14/15(e)(2). While important, this mandate is largely superfluous in that biometric data is now treated as ''personal information'' in many states' data breach notification laws, including Illinois. As such, the unauthorized access to stored biometric information will trigger notification obligations in many states, and organizations storing such data must be, at a minimum, using industry-standard data security mechanisms to protect biometric data. In addition, the FTC has issued guidance that it expects biometric information to be protected through ''privacy by design'' in the same way as other types of personally identifiable information. Federal Trade Commission, *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*, (Oct. 22, 2012).

BIPA Litigation To date, class action plaintiffs have focused on allegations that organizations failed to comply with BIPA's notice and consent mandates. Two types of fact patterns have emerged: 1) improper use of facial recognition technology; and 2) improper collection and use of fingerprints, primarily in the employment context.

Facial Recognition Litigation

Suits alleging a violation of BIPA for the improper collection of facial geometries have centered around technology companies, such as social media and photo-sharing websites. *See, e.g.*, *Norberg v. Shutterfly, Inc.*, No. 1:15-cv-5351 (N.D. Ill.); *Martinez et al. v. Snapchat Inc.*, No. 2:16-cv-05182 (C.D. Cal.); *Licata v. Facebook, Inc.*, Nos. 3:15-cv-03748, 3:15-cv-03749, and 3:15-cv-03747 (N.D. Cal.). In each of these cases, the plaintiffs allege that the defendant used facial recognition software to collect and store the biometric identifiers of individuals in uploaded photos without first obtaining their consent, as required by BIPA. For instance, in *Norberg v. Shutterfly*, the plaintiff, who was not a Shutterfly customer and did not have a Shutterfly account, discovered that he had been tagged in a picture on the website by a friend. He then brought suit, alleging that, through the process of storing and tagging the picture, Shutterfly recorded his facial geometric identifiers without his consent.

The defense in these types of cases has centered on whether the scan of a photograph, rather than the scan of a person's face directly, can constitute a biometric identifier. The defendants claim that obtaining facial recognition from a photograph is merely collecting information *derived* from biometric identifiers rather than the identifiers themselves, and the practice is thus exempt from BIPA. However, thus far, the courts have rejected this argument. In doing so, the courts have generally held that biometric identifiers, as used in BIPA, refer to the measurements themselves rather than to medium through which the measurements are collected.

Fingerprint Litigation

Dozens of complaints have also been filed alleging that companies failed to provide notice or obtain consent before collecting individuals' fingerprints. This complaint typically arises in the employment context, where hourly employees use their fingerprints to clock in and out of work. For instance, in a recent complaint filed against Roundy's Supermarkets, which operate the Mariano's chain of grocery stores, the plaintiffs allege:

''Plaintiff arrived for work, and when he left or clocked in or out of work, at relevant times during his employment, Roundy's required him to submit his fingerprint to its timekeeping computer system. The system captured, collected, extracted, recorded, stored, and used his biometrics. Roundy's further required Plaintiff to scan his fingerprint and swipe an identification card in order to use the biometric system, so that the timekeeping system captured, collected and matched his fingerprint biometrics, and associated his biometrics with his identity.'' *See, e.g.*, Complaint, *Baron v. Roundy's Supermarkets, Inc.*, 2017-CH-03281 at ¶ 29 (Cook Cty. March 7, 2017) *removed Baron v. Roundy's Supermarkets, Inc.*, No. 17-03588 (N.D. Ill. May 11, 2017).

With such an expansive view of the types of actions that constitute a violation of BIPA, combined with the large potential pools of plaintiffs for companies with operations in Illinois, the stakes are large. For instance, in the *Roundy's* case, in noting that the matter qualified for removal under the Class Action Fairness Act, with its requirement that the amount in controversy exceed $5,000,000, counsel for the defendant notes that the supermarket ''currently has over 10,000 employees who work in grocery stores located in the State of Illinois and who have clocked in and clocked out of their shifts using biometric technology [along with] several hundred or thousand former employees. . .'' resulting in a class recovery of over $7,500,000 if 75% of the potential class participates in the suit. Notice of Removal, *Baron v. Roundy's Supermarkets, Inc.*, No. 17-03588 at ¶ 15 (N.D. Ill. May 11, 2017). Moreover, this number may be conservative as it assumes that the plaintiffs will not be able to demonstrate intentional violations of BIPA (which would raise the penalty from $1,000 per violation to $5,000) and that the company only committed one ''violation'' with respect to each individual plaintiff.

   ISSN 1529-0115

In one of the few resolutions of BIPA litigation to date, L.A. Tan settled with a class of plaintiffs in December 2016 for $1.5 million, agreeing to pay $600,000 in attorney's fees and settling with each class member for between $125 and $150. *Sekura v. LA Tan Enterprises*, No. 2015-ch-16694 (Cook Cty. Dec. 1, 2016). It remains to be seen what types of settlements other plaintiffs' attorneys will be able to extract from companies that have not complied with BIPA's requirements.

Litigation Defenses and Responses While most of the litigation in this space is still in its fledgling stages, several common defenses have arisen, with varying degrees of success.

Article III Standing under Spokeo

First, BIPA defendants may argue that the ''harm'' suffered by the plaintiffs is too abstract or immaterial to give rise to Article III standing under the Supreme Court's ruling in *Spokeo v. Robins*. 136 S. Ct. 1540 (2016) (holding that plaintiffs alleging violations of statutes that contain a private right of action and statutory damages must allege a ''concrete and particularized harm''). In that ruling, the Court held that Article III standing requires a concrete injury even in the context of a statutory violation. In several instances, courts have found that technical violations of BIPA do not give rise to standing without evidence of actual harm. For instance, in *McCollough v. Smarte Carte Inc.*, the plaintiffs brought suit under BIPA alleging that the defendant improperly collected and used customers' fingerprints as ''keys'' for public lockers without prior written consent. No. 16-cv-03777 (N.D. Ill. Aug. 1, 2016). In granting the defendant's motion to dismiss, the court held that the plaintiffs' had failed to allege an actual and specific injury under *Spokeo* and that a mere technical or procedural violation of BIPA was insufficient to grant standing without a showing of an actual injury. Recently, a decision by the Second Circuit upheld a lower court's ruling in line with *McCollough*, finding that a technical violation of BIPA could not satisfy *Spokeo*.

However, more recently in *Monroy v. Shutterfly Inc.*, the court held that the mere invasion of privacy associated with the defendant's collection of biometric information without the plaintiffs' knowledge or consent was sufficient injury-in-fact to give rise to standing. No. 16-cv-10984 (N.D. Ill. Sept. 15, 2017). In doing so, the court distinguished its ruling from *McCullough* in holding that unlike in that case, where customers knowingly and voluntarily provided their fingerprints to the defendant, the defendant in *Monroy* surreptitiously collected and stored the plaintiffs' facial scans without their knowledge or consent. As such, the court found that the plaintiffs could credibly allege and invasion of privacy in addition to any technical violation of BIPA.

As these decisions indicate, there is disagreement among the courts regarding how to interpret *Spokeo* in the privacy context. Similar arguments relating to data breaches have caused a circuit split that may be taken up by the Supreme Court in the near future, as a writ of certiorari was recently filed for the D.C. Circuit Court of Appeal's decision in *Attias v. CareFirst*. *Compare In re SuperValu Customer Data Security Breach Litigation* (8th Cir. 2017) (finding that plaintiffs who had not yet suffered fraudulent charges or identity theft following a breach could not sufficiently allege a substantial risk of future injury); *Whalen v. Michaels Stores* (2d Cir. May 2017) (same); *Beck v. McDonald* (4th Cir. 2017) (same) *with Attias v. CareFirst* No. 16-710 (D.C. Cir. 2017) (finding the increased likelihood of harm from a data breach sufficient injury to give rise to standing); *Galaria v. Nationwide Mut. Insur. Co.* (6th Cir. 2016) (same); *In re: Horizon Healthcare Services Inc. Data Breach Litigation* (3d Cir. 2017) (same).

Standing Under Illinois State Law

One drawback to the *Spokeo* standing argument is that it applies, on its face, only in federal court. *See Asarco, Inc. v. Kadish*, 490 U.S. 605, 617 (1989) (''[T]he constraints of Article III do not apply to state courts, and accordingly the state courts are not bound by the limitations of a case or controversy or other federal rules of justiciability even when they address issues of federal law.''). While corporate defendants often prefer federal to state court, and remove litigation to federal court wherever possible, seeking a dismissal for lack of subject matter jurisdiction under *Spokeo* after successfully removing litigation to federal court may be problematic. While subject matter jurisdiction under Article III can be raised at any time, including after remand, defendants who use *Spokeo* in an attempt to obtain dismissal before a district court after having argued for removal risk facing judicial displeasure. *See Grupo Dataflux v. Atlas Global Grp., L.P.*, 541 U.S. 567, 576 (2004) (''A litigant generally may raise a court's lack of subject-matter jurisdiction at any time in the same civil action, even initially at the highest appellate instance.''). In one extreme instance, a district court judge remanded a case back to state court while also awarding the plaintiff attorneys' fees and expenses for the related motion practice. *Mocek v. Allsaints USA Ltd.*, No. 16 C 8484 (N.D. Ill. Dec. 7, 2016). More commonly, district court judges merely remand the litigation back to state court. *See*, *e.g.*, *In re Michaels Stores, Inc.*, No. 14-7563 (KM) (JBC) (D.N.J. Jan. 24, 2017); *Patton v. Experian Data Corp.*, No. SACV 15-1871 JVS (PLAx) (C.D. Cal. May 6, 2016).

While Article III standing principles may not authoritatively control state court disputes, Illinois law generally mimics federal law in requiring a certain degree of concreteness for standing. For instance, in the data breach context, Illinois courts have followed some federal jurisdiction cases—with explicit citations to those federal decisions, including the Supreme Court's decision in *Clapper*—in finding that the mere increased risk of harm from a breach is insufficient for standing without a showing of actual harm. *Maglio v. Advocate Health & Hosps. Corp.*, 2015 IL App (2d) 140782, ¶ 26, 40 N.E.3d 746, 754, *appeal denied*, 39 N.E.3d 1003 (Ill. 2015) (''As plaintiffs here have not alleged that their personal information has actually been used or that they have been victims of identity theft or fraud, the arguably increased risk of such acts as a result of Advocate's data breach is insufficient to confer standing as that concept is applied in federal cases.'').

Statutory Standing Under BIPA – Aggrieved Injury

Beyond constitutional standing arguments, BIPA itself also requires some form of actual harm. Section 20 of BIPA states that ''[a]ny person *aggrieved by a violation of this Act* shall have a right of action. . . .'' 740 ILCS 14/20 (emphasis added). Thus, similar to the Article III standing analysis discussed above, the BIPA statute itself requires the plaintiff to allege some harm, loss, or injury beyond a mere technical violation. While this remains an unsettled area of the law and courts

have reached opposite conclusions, early decisions, at both the federal and state level, indicate that the courts read ''aggrieved'' to require an actual injury. For instance, in the *McCollough* decision discussed above, the court held that ''it appears, that by limiting the right to sue to persons aggrieved by a violation of the act, the Illinois legislature intended to include only persons having suffered an injury from a violation as 'aggrieved.' '' No. 16-C-03777 at 7 (N.D. Ill. Aug. 1, 2016). More recently, in *Rosenbach v. Six Flags Entertainment Corp.*, 2017 IL App (2) 170317, an Illinois appellate court weighed in on BIPA for the first time. In that case, the appellate court held that ''[i]f a person alleges only a technical violation of the Act without alleging any injury or adverse effect, then he or she is not aggrieved and may not recover under any of the provisions in section 20.'' *Rosenbach*, 2017 IL App (2) 170317 at ¶ 28. In reaching this conclusion, the court engaged in significant statutory analysis as to the meaning of ''aggrieved'' and also looked to the *McCollough* decision. While this decision clearly articulates the standard under BIPA that a person must suffer actual harm in order to be ''aggrieved'' under BIPA, and thus qualify for statutory standing, the court also noted that this harm must not be pecuniary, which plaintiffs may interpret as an invitation to rely upon allegations of non-monetary forms of harm such as emotional distress or an invasion of privacy. *Id.* Nonetheless, this decision is an important win for BIPA defendants seeking to dismiss BIPA class actions at an early stage of litigation.

The Constitutionality of BIPA

In addition, the constitutionality of BIPA has been called into question by several defendants. For instance, in *In re Facebook Biometric Info. Privacy Litig.*, Facebook has argued that BIPA constitutes an unconstitutional burden on inner-state commerce. No. 15-cv-03747 (N.D. Cal.). The courts have yet to issue a definitive ruling on the constitutionality of BIPA.

Personal Jurisdiction

Despite being an Illinois law, the plaintiffs' bar has been aggressive in pursuing organizations based outside of Illinois, or with only minimal operations in the state. This has naturally given rise to disputes over personal jurisdiction. These arguments typically arrive in the context of website operators without a physical presence in the state.

Does the Data in Question Constitute Biometric Information?

Finally, as discussed in more detail above, the scope of what is considered a ''biometric identifier'' is largely untested and, especially in the facial recognition context, several defendants have argued that the information at issue falls outside of BIPA. While this issue has been discussed most frequently in the facial recognition context, it is likely to expand as BIPA litigation continues to expand. For instance, in the fingerprint context, some complaints allege that the storing of mathematical representations of fingerprints fall under BIPA's definition of biometric information, while defendants are likely to argue that such representations are merely derivatives of biometric information and thus fall outside of BIPA.

What Statute of Limitation Applies to BIPA? One additional area of debate surrounding BIPA is the appropriate statute of limitations period. The statute itself does not provide for a limitations period, and there are arguments that several different lengths are appropriate under Illinois state law.

First, the appropriate limitations period could be one year under 735 ILCS 5/13-201, which applies to certain privacy rights such as ''slander, libel, and publication of matter violating the right of privacy.'' In addition, the Illinois Right to Privacy Act—which, like BIPA, does not have a statutory limitations period—has been interpreted as incorporating a one year limitation period. *See Blair v. Nevada Landing Partnership,* 369 Ill. App. 3d 318 (2006). However, Illinois courts have held that Section 12-201's application to all ''privacy torts'' is limited only to those privacy torts involving ''publication,'' as specifically listed in the statute. *Johnson v. Northshore Univ. Judge Presiding Healthsystem*, No. 1-10-0399 (Ill. App. Ct. Mar. 31, 2011).

Second, there is support for a two-year limitations period under 735 ILCS 5/13-202, which applies to both personal injury suits and statutes which provide for a ''statutory penalty.'' BIPA claims are also, in some respects, similar to personal injury suits sounding in negligence, and thus it is possible that Section 5-202 is appropriate. In addition, one could argue that that BIPA's statutory damages—which aware either $1,000 or $5,000 *or* actual damages—constitute a statutory penalty, which would trigger the two-year period under 12-202. Third, litigants may argue that the courts should look to the Illinois Consumer Fraud and Deceptive Business Practices Act, which provides for a three-year statute of limitations. 815 ILCS 505/10a(e). This law broadly applies to other instances of improper data collection and usage, including claims brought under the Illinois Personal Information Protection Act, the state's data breach notification law. This argument is bolstered by the fact that BIPA seems to anticipate a three-year period in that it allows for a record retention period of three years since an organization's last interaction with an individual.740 ILCS 14/15.

Finally, in the event that BIPA does not fit with any of the options listed above, plaintiffs may ask courts to apply Illinois' ''catch-all'' statute of limitation period of five years to the statute. 735 ILCS 5/13-205. As companies continue to litigate BIPA, courts will surely resolve the open questions surrounding which limitations period applies, as the answer to that question could have a significant impact on the potential class members and damages.

Conclusion Until the courts show a willingness to interpret BIPA narrowly and dismiss class actions at an early stage, BIPA litigation is likely here to stay. For this reason, any organization collecting or using biometric data—in either the consumer or employment context—is well advised to closely examine its privacy practices. While BIPA was largely ignored for the first eight years of its existence, compliance with its requirements has become an expensive proposition. Moreover, biometric privacy is likely to continue growing in scope as more companies begin to use this technology and as more jurisdictions pass biometric-focused legislation.

   ISSN 1529-0115