PORZIO

BROMBERG&NEWMAN P.C.

Class Action Update

NINTH CIRCUIT HOLDS VIOLATION OF ILLINOIS BIOMETRIC INFORMATION PRIVACY ACT CONVEYS ARTICLE III STANDING IN CLASS ACTION

Authored by: Steven P. Benenson[1]

On August 9, 2019, a Ninth Circuit Court of Appeals panel affirmed a California district court's order permitting a class action against Facebook for allegedly using facial-recognition technology without users' written consent or a data retention policy in violation of Illinois' Biometric Information Privacy Act ("BIPA"). This is the first federal court of appeals decision recognizing Article III standing under BIPA, which will encourage more of these cases and may affect other data privacy litigation.

The BIPA requires companies to disclose the collection of biometric data and its purpose, to securely store it, and to obtain written consent. 740 ILSC 14/1, §15. Under the Act, "[a]ny person aggrieved by a violation" is afforded a private right of action against the "offending party" and "may recover for each violation" the greater of liquidated damages up to $5,000 or actual damages, attorneys' fees and costs, and injunctive relief. *Id.* §20. In enacting BIPA, the Illinois General Assembly focused on the uniqueness and inalterability of biometric markers such as one's face, retina, fingerprints, and voice prints and the risk that "once compromised, the individual has no recourse, [and] is at heightened risk for identity theft. . . ." *Id.* §5.

As we discussed in a prior update, the federal and state courts have not reached consensus on whether plaintiffs in data privacy class actions have standing absent concrete and particularized harm that is actual or imminent. Although the Illinois Supreme Court earlier this year rejected the argument that a mere technical violation of BIPA without alleging some injury or adverse impact is fatal to a class action claim, *Rosenbach v. Six Flags Entertainment Corp.*,–– N.E.3d ––; 2019 WL 323902 (Il. Jan. 25, 2019), it was not clear if the federal courts would embrace this approach.

In *Patel v. Facebook,* ––F.3d––, 2019 WL 3727424 (9th Cir. Aug. 8, 2019), Facebook had launched a feature called "Tag Suggestions," which uses facial recognition technology to analyze whether the user's friends appear in uploaded photos, identifies that person by name and includes a link to his or her on-line profile. *Id.* *1. In reviewing the district court's denial of defendant's motion to dismiss on standing grounds, the Court of Appeals adopted a traditional two-prong analysis: 1) whether the BIPA protected the plaintiff's concrete interests (as opposed to purely procedural rights), and 2) whether the alleged procedural violations actually harm, or present a material risk of harm, to such interest. *Id.* *4.

First, the Court of Appeals found that BIPA protects privacy rights long recognized in common law and constitutional jurisprudence. *Id.* *4-5. The Ninth Circuit noted that once a digital face template is created, Facebook could use it to identify that individual in the hundreds of millions of photos uploaded to the site daily, determine when that person was at a specific location through geotagging and identify the individual's friends who also appear in the photo. The court held that use of facial recognition technology without consent "invades an individual's private affairs and concrete interests" and is actionable at common law. *Id.* *5. The Illinois Supreme Court's *Rosenbach* decision further supported the conclusion that an individual is aggrieved by violations of

[1]Steven P. Benenson is a senior litigation principal with Porzio, Bromberg & Newman, PC, in New York City and Morristown, New Jersey, and chairs the firm's complex litigation practice. He has been defending class actions for 35 years in diverse industries and businesses in state and federal trial and appellate courts across the country. He is recognized in *Best Lawyers in America*, in Mass Tort Litigation/Class Actions – Defendant, served as the Program Chair of the 2016 ABA National Class Action Symposium and co-authored the New Jersey chapter of the ABA's *A Practitioner's Guide to Class Actions*. Steve is a frequent presenter and author on class action topics.

BIPA because it constitutes "'the invasion, impairment or denial of the statutory rights'" of any person whose biometric information is subject to the breach. *Id.* *6 (*citing* 2019 WL 323902 at *7).

As to the second prong, the Ninth Circuit also concluded that "[b]ecause the privacy right protected by BIPA is the right not to be subject to the collection and use of such biometric data, Facebook's alleged violation of these statutory requirements would necessarily violate the plaintiff's substantive privacy interests." *Id.* *6. The Court of Appeals found that "the plaintiffs alleged a concrete injury-in-fact sufficient to confer Article III standing." *Id.*

The Ninth Circuit also rejected Facebook's argument that Illinois extraterritoriality doctrine precluded application of BIPA where the biometric technology was employed on servers located outside the state. Noting that BIPA is silent on this score, the court concluded 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 occurred outside the state." This issue could be decided on a class-wide basis without mini-trials that would defeat certification. *Id.* 7. The Court of Appeals also held that the potential of substantial, class-wide damages would not make individual actions superior, finding that "nothing in the text or legislative history of BIPA indicates that a large statutory damages award would be contrary to the intent of the General Assembly." *Id.* *8.

Given the broad view of standing espoused by the *Rosenbach* and *Patel* courts, and the rejection of Facebook's extraterritoriality defense in the latter case, we expect a substantial uptick in BIPA cases in the Ninth Circuit. It remains to be seen whether other federal appeals courts will follow Patel in conferring Article III standing in BIPA class actions. Outside of this context, other data privacy class claimants will undoubtedly argue that mere statutory or common law violations, without allegations of actual harm, should suffice and that the potential for enormous monetary damages is not an impediment to class certification. Companies conducting or facilitating ecommerce in Illinois that capture biometric data without complying with BIPA could invite claims in the federal courts in Illinois or where their corporate headquarters or data centers are located.