THOMSON REUTERS
Westlaw®

Recent developments under BIPA: Examining *Spokeo's* impact and more

By Torsten M. Kracht, Esq., Michael J. Mueller, Esq., Lisa J. Sotto, Esq., and Bennett Sooy, Esq.
Hunton Andrews Kurth LLP

JUNE 1, 2018

In February the U.S. District Court for the Northern District of California ruled in *Patel v. Facebook Inc.*[1] that the plaintiffs' allegations that Facebook violated the statutory notice-and-consent procedures of Illinois' Biometric Information Protection Act[2] were enough to state a claim of an intangible harm that constitutes a concrete injury-in-fact sufficient to confer Article III standing.

The court has since certified the case as a class action, finding that it is possible for the class members to show in a unified way that they are "aggrieved" under BIPA because a violation of the statute is the only injury they must prove.[3]

In denying Facebook's motion to dismiss, the District Court found that BIPA vested in Illinois residents the right to control their biometric information by requiring notice before collection and the ability to withhold consent.

By creating these protections, Illinois lawmakers codified a right of privacy in personal biometric information. As a result, a violation of the procedural rights granted by BIPA necessarily amounts to a concrete injury because it infringes on the privacy rights protected by the statute.

As the U.S. Supreme Court recognized in *Spokeo Inc. v. Robins*, violation of statutory procedural rights can be sufficient to confer standing.[4] Therefore, the class plaintiffs were not required, as Facebook argued, to show any additional "real-world harms."

The ruling on standing foreshadowed the granting of class certification, as the court applied the same logic — that violation of the statute constitutes a concrete injury — to find that class members could rely on common proof to show that they were harmed by Facebook's collection of their biometric information.

The court also interpreted BIPA's statutory language that a person "aggrieved" by a violation has a private right of action as not requiring the pleading of additional "actual injury," so individual issues would not predominate.

That is not to say that there aren't significant factual issues in finding that Facebook violated BIPA, as the District Court emphasized when it recently denied the parties' cross-motions for summary judgment.[5]

The case is now set to proceed to trial in July. The certified class is slightly narrower than the plaintiffs' initial proposal of all Illinois users appearing in a photograph uploaded to Facebook. Instead, it includes only Illinois users for whom Facebook created and stored a face template.

Facebook has petitioned the 9th U.S. Circuit Court of Appeals for review of the certification ruling. In the meantime, there appears to be a bright path to class certification for those whose biometric information was captured and stored after June 7, 2011, in violation of BIPA's plain language.

That path may be dimmed by a proposed amendment to the statute. If it becomes law, the amendment will exempt private entities from BIPA if:

(1) The biometric information is used exclusively for employment, human resources, fraud prevention or security purposes;

(2) The company does not profit from the information collected; or

(3) The company protects biometric information in the same way it protects its own confidential information.[6]

Even if it is not applied retroactively,[7] the amendment could wipe out litigation involving employers that use fingerprint-capture technology relating to access control and employee time-keeping systems. This type of case currently comprises the bulk of BIPA class litigation.

STATUTORY DEVELOPMENTS

Though Illinois remains the only state where a private right of action exists for violation of biometric data privacy laws, in recent months two more states have introduced legislation that could expand the availability of BIPA-like claims.

In New York, A.B. 9793 provides a private right of action against private entities with statutory damages of $1,000 for negligent violations and $5,000 for intentional or reckless violations, injunctive relief and attorney fees and costs, including expert witness fees and other litigation expenses.

In Indiana, S.B. 248 makes violations actionable under the Indiana Deceptive Consumer Sales Act and subject to statutory damages of $500, which may be increased up to $1,000 for willful violations, and attorney fees.

Other states have also taken legislative action in this area. Of the bills creating a private right of action introduced last year in Alaska, Michigan, Montana and New Hampshire, New Hampshire's bill moved closer to becoming law when the state House passed it in January.[8] The legislation is currently being considered in the state Senate.

The Montana bill died in the standing committee.[9] And Texas remains the only state other than Illinois with a statute regulating the collection of biometric information that provides for monetary penalties.[10]

GOOGLE DENIES ACCESS IN REGULATED STATES

Google made its own headlines early this year when the selfie feature in its Arts & Culture app, which matched users' faces with works of art bearing a resemblance, became a cultural phenomenon, and the company seemingly took a stance on BIPA laws.

Users in Illinois and Texas were dismayed to discover that the function was not available to them, which Google confirmed was intentional.[11] Google withheld the functionality from users in Illinois and Texas even though the app complied with those states' notice and consent requirements.

While voters can hardly be expected to cry foul to their representatives over missing out on the latest selfie craze, Google's clear statement that states with penalties can be avoided raises what could become a serious issue as more products with biometric-enabled features are introduced.

The time may come when citizens in these states will have to choose which they value more: an intangible right to privacy, as defined by lawmakers in the state capitol, or having access to new tech developments.

NOTES

[1] 290 F. Supp. 3d 948 (N.D. Cal. 2018).

[2] 740 Ill. Comp. Stat. 14/1 (2008).

[3] *In re Facebook Biometric Info. Privacy Litig.,* No. 15-cv-3747-JD, 2018 WL 1794295 (N.D. Cal. Apr. 16, 2018).

[4] 136 S. Ct. 1540, 1549 (2016).

[5] *In re Facebook,* 2018 WL 2197546 (N.D. Cal. May 14, 2018).

[6] H.B. 5103, 100th Gen. Assembly (Ill. 2018).

[7] The Illinois Supreme Court has adopted the Supreme Court's approach in *Landgraf v. USI Film Products,* 511 U.S. 244 (1994), and will "consider whether retroactive application of the new statute will impair rights a party possessed when acting, increases a party's liability for past conduct, or impose new duties with respect to transactions already completed." *Doe A. v. Diocese of Dallas,* 917 N.E.2d 475, 482 (Ill. 2009).

[8] H.B. 523, 2017 Sess. (N.H. 2017).

[9] H.B. 518, 65th Leg., Reg. Sess. (Mont. 2017).

[10] The Texas Statute on the Capture or Use of Biometric Identifier, Tex. Bus. & Com. Code Ann. § 503.001, provides for enforcement by the attorney general and civil penalties of up to $25,000 per violation.

[11] *See* Dianne de Guzman, *Google App Finds Museum Doppelgangers for Selfie-Takers Around the World,* SFGate (Jan. 14, 2018), https://bit.ly/2s8279X.

This article first appeared in the June 1, 2018, edition of Westlaw Journal Computer & Internet.

ABOUT THE AUTHORS

(L-R) **Torsten M. Kracht** is a partner at **Hunton Andrews Kurth LLP** in Washington, where he represents clients from the U.S. and abroad in complex litigation and arbitration. He can be reached at tkracht@huntonak.com. **Michael J. Mueller** is a partner at the firm in Washington, and he handles class actions and other complex cases. He can be reached at mmueller@huntonak.com. **Lisa J. Sotto** is the managing partner of the firm's New York office and chair of its global privacy and cybersecurity practice. She can be reached at lsotto@huntonak.com. **Bennett Sooy** is a litigation associate at the firm in Washington. He can be reached at bsooy@huntonak.com. Special thanks to librarians Elizabeth Collins and Jonathan Hartnett.