By Kamran Salour

On Monday, the Northern District of California issued a ruling denying Facebook's motion to dismiss for lack of subject matter jurisdiction a biometric-privacy-based class action. *In re Facebook Biometric Information Privacy Litigation*, 3:15-cv-03747 (N.D. Cal., Feb. 26, 2018). The ruling will likely have long-term implications for a company that collects, captures or stores biometric information.

A company that collects, captures or stores biometric information already has sparse guidance on how to navigate the largely unchartered biometric privacy legal landscape. Only three states — Illinois, Texas and Washington — have statutes protecting biometric information. And only the Illinois statute, the Biometric Information Privacy Act, allows for a private right of action. Unsurprisingly, BIPA is the only one to have undergone judicial interpretation.

The latest judicial interpretation of BIPA — this week's ruling — generated a new permutation that a company must now consider: a plaintiff may still have standing to assert a cause of action under BIPA notwithstanding that plaintiff's failure to allege a concrete injury-in-fact resulting from that violation.

What Is BIPA?

The Illinois legislature enacted BIPA in 2008. The act generally requires that before an entity collects, captures, or stores a consumer's biometric information that entity must first: (i) inform the consumer in writing that the consumer's biometric information is being collected or stored and the specific purpose and duration of the collection, storage, or usage; and (ii) receive an executed written release from the consumer consenting to the collection, capture, or usage. BIPA authorizes a minimum $1,000 statutory penalty, per violation, for failure to comply with these notice and consent provisions.

Lack of Standing Defense

As an entity's collection, storage and usage of a consumer's biometric information became more pervasive, so too did class actions alleging violations of BIPA's notice and consent provisions. BIPA's $1,000 per violation penalty undoubtedly sparked a class action influx.

Serendipitously, soon after the influx of BIPA class actions, the U.S. Supreme Court issued its decision in *Spokeo v. Robins*, 136 S. Ct. 1540 (2016). While the Supreme Court only evaluated whether Robins had standing to maintain his action in federal court alleging that Spokeo violated the Fair Credit Reporting Act, and only held that the 9th U.S. Circuit Court of Appeals' Article III analysis was incomplete, the decision was widely construed more broadly: that a bare procedural violation alone — without alleging a resulting concrete injury-in-fact — is insufficient to confer Article III standing.

Soon after *Spokeo*, an entity defending a BIPA class action filed in federal court relied on *Spokeo* to seek dismissal for lack of subject matter jurisdiction. *See, e.g.*, *McCollough v. Smarte Carte, Inc.*, 16 C 03777, (N.D. Ill. Aug. 1, 2016); *Vigil v. Take-Two Interactive Software, Inc.*, 235 F. Supp. 3d 499 (S.D.N.Y. 2017).

In *Smarte Carte*, plaintiff McCollough filed a class action against Smarte Carte, owner and operator of electronic lockers that lock and unlock using the locker renter's fingerprint. McCollough's complaint alleged that Smarte Carte violated BIPA because it collected and retained her biometric information (her fingerprint) without complying with BIPA's notice and consent requirements. McCollough did not allege a resulting injury-in-fact. Smarte Carte filed a motion to dismiss for lack of standing; the district court, relying on *Spokeo*, granted Smarte Carte's motion.

In *Take-Two*, the plaintiffs filed a class action against Take-Two, the maker of a videogame that allows a player to create a personalized avatar for in-game use. The plaintiffs alleged that Take-Tow violated BIPA because it collected and retained biometric information (a player's face scan) without complying with BIPA's notice and consent provisions. The plaintiffs did not allege any resulting injury-in-fact. Take-Two

filed a motion to dismiss for lack of standing, which the district court, relying on *Spokeo,* granted. The 2nd Circuit affirmed.

Based on *Smarte Carte* and *Take-Two,* it would appear that an entity that collects, stores or uses biometric information can rely on *Spokeo* to dismiss for lack of subject matter jurisdiction a class action filed in federal court alleging violations of BIPA if the complaint fails to allege a resulting injury-in-fact. This, as Facebook just learned, is not entirely true.

The *Facebook* plaintiffs alleged that Facebook violated BIPA's notice and consent requirements when it captured and stored their biometric information (face scans) in connection with Facebook's "Tag Suggestions" feature, after the plaintiffs uploaded their photographs onto Facebook. The plaintiffs did not allege any resulting harm, so Facebook, relying on *Spokeo,* sought to dismiss the plaintiffs' complaint for lack of subject matter jurisdiction.

The court denied Facebook's motion. The court analyzed BIPA's plain language and concluded that the Illinois legislature codified a right of privacy in biometric information, and that the legislature empowered a consumer to control their biometric information by imposing notice and consent requirements on an entity that collects that information. Bypassing BIPA's notice and consent requirements, denies a consumer the right of privacy in biometric information. A violation of BIPA's notice and consent requirements is therefore an intangible harm that constitutes a concrete injury-in-fact necessary for Article III standing.

The court also distinguished *Smarte Carte* and *Take-Two*. In *Smarte Carte*, McCollough understood that Smarte Carte would collect and store her fingerprint; how else could McCollough lock and unlock the locker? Similarly, the plaintiffs in *Take-Two* understood that Take-Two would at least collect a player's face scan; creating a personal avatar requires a player to face a camera for nearly 15 minutes and acknowledge that Take-Two may record that player's face scan. Conversely, the *Facebook* plaintiffs did not understand that Facebook would collect and store their biometric information when they uploaded photographs onto Facebook.

The implications of this ruling are encompassing. For the plaintiffs' bar, this ruling will likely encourage more BIPA class actions. For the defense bar, this ruling presents another obstacle in navigating the biometric legal landscape. And for an entity that engages in activity that a consumer understands requires the collection, storage, or use of biometric information, it arguably creates an incentive not to comply with BIPA's notice and consent requirements.

Kamran Salour is an attorney with Callahan & Blaine in Santa Ana.