LOEB & LOEB LLP

Privacy

OCTOBER 2018

Amid Flood of Suits and Conflicting BIPA Rulings, Illinois Supreme Court, Legislature Weigh In

In March, we alerted readers to the flurry of class action litigation asserting claims under Illinois' Biometric Information Protection Act based on the collection of biometric data, including through the use of fingerprint scanning and facial recognition software.

We also noted the precarious legal landscape regarding what plaintiffs need to plead for an "injury in fact" to establish standing under the Act –in particular the apparent split in decisions. In the recent Illinois Appellate Court ruling in *Rosenbach v. Six Flags Entertainment Corp and Great America LLC*, the court held that an allegation of only a technical violation of the Act, without alleging any injury or adverse effect, is not sufficient to confer standing. In contrast, a recent California district court decision concluded that a violation of the BIPA notice and consent procedures "infringes the very privacy rights the Illinois legislature sought to protect … quintessentially an intangible harm that constitutes a concrete injury in fact."

Since then, the volume of lawsuits has only increased, as has the uncertainty as to what plaintiffs have to allege on the element of injury to get past the standing threshold and keep their cases in court.

Some answers (hopefully) may be on the horizon, as both the Illinois Supreme Court and the Illinois legislature are reviewing the scope and breadth of the statute.

Recent split decisions interpreting BIPA

Over the past six months, several courts have addressed the standing issue in Illinois, indicating an emerging trend that allows plaintiffs to get past the initial standing threshold by pleading the sharing of data with a third-party vendor. For example, in *Goings v. UGN, Inc.*, Judge Bucklo in the Northern District of Illinois remanded a case brought under BIPA back to state court, noting that the plaintiff-employee had failed to identify any concrete harm from his employers' requirement that employees use fingerprint and handprint scans to clock in and out and specifically citing the lack of allegation that data had been shared with any third-party without consent. In contrast, in *Dixon v. Washington and Jane Smith Community, et al.*, Judge Kennelly (in a 38-page opinion) declined to dismiss claims against a senior living center and its time clock vendor over the scanning of employee fingerprints, holding that the senior center had shared information with the time clock vendor without informing the employees it was doing so. The *Dixon* court distinguished the allegations from *Rosenbach* noting: "[i]n this case, in addition to alleging what might accurately be characterized as 'bare procedural violations' of BIPA, Dixon also has alleged that Smith disclosed her fingerprint data to Kronos without her knowledge and that the defendants violated her right to privacy in her biometric information — the very right that the drafters of BIPA sought to protect."

The Illinois Supreme Court steps in to resolve the uncertainty — maybe…

The Illinois Supreme Court in May accepted plaintiff's appeal in the *Rosenbach* case. The question presented, as framed by counsel for plaintiff, is whether a party is an "aggrieved party" (i.e., has standing) if the only injury alleged is the collection of data without the proper disclosures and consent. Since then, notable "friends of the court," or amici, have weighed in. For example, on plaintiff's side, the American Civil Liberties Union, joined by the Center for Democracy and Technology, Illinois PIRG, the Chicago Alliance Against Sexual Exploitation, Electronic Frontier Foundation and the Lucy Parsons Lab have submitted a brief arguing that significant risk and harm occur from the collection of biometric data without consent and disclosure, and stressing the need to encourage private enforcement of the statute. On defendant's behalf, briefs have been submitted by the Illinois Chamber of Commerce, the Internet Association and the Illinois Restaurant Association, as well as a collective filing by the Illinois Retail Merchants Association, National Retail Federation and National Federation of Independent Business.

What is most notable — and perhaps troubling if we're looking for some certainty in these cases — is that the court's review of the *Rosenbach* decision does not appear broad enough to address the allegations that now seem to be slipping through at the motion-to-dismiss stage (as in the Dixon case). The supreme court is technically limited to the facts and question certified by the lower appellate court — the lack of consent related to collection — not the issue of sharing data with a contracted third party. With that said, this has not stopped several of the amicus from attempting to broaden the court's review, in essence arguing that the court must first define "aggrieved" before it can answer the question presented. In doing so, at least one amicus argued that no inherent privacy right exists in fingerprints, handprints or facial scans and, therefore, employees who knowingly and willingly use scanners cannot be "aggrieved" under the statute.

Despite these efforts — and the efforts of other parties that continue to seek leave to file amicus briefs with the court — a strong chance exists that the court may affirm the *Rosenbach* decision — which simply states a person must allege actual injury and not just a technical violation — and leave unanswered the broader question of what a plaintiff must allege to demonstrate actual injury under the statute.

The matter is now fully briefed, as plaintiff-appellant Stacey Rosenbach filed her reply brief at the end of September. As of now, the court has not scheduled any argument on the case.

Help from the legislature?

Several other amici utilized their briefs to bemoan the rampant unfairness of the "no injury" class action, especially as it relates to employers in the context of the BIPA. As the Illinois Chamber of Commerce noted, an Illinois business utilizing biometric technology with only 20 employees could be exposed to $100 million in damages if they had utilized a scanner over the past five years. In an effort to balance the real concerns identified by the ACLU and other digital privacy advocates with the potentially devastating effect the statute could have on companies doing business in Illinois, the Senate has introduced a bill, Senate Bill 3053, that would, according to the Senate summary, amend the Biometric Information Privacy Act so that "nothing in the Act shall be deemed to apply to a private entity collecting, storing, or transmitting biometric information if: (i) the biometric information is used exclusively for employment, human resources, fraud prevention, or security purposes; (ii) the private entity does not sell, lease, trade, or similarly profit from the biometric identifier or biometric information collected; or (iii) the private entity stores, transmits, and protects the biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information." Under the Illinois Senate rules, the Senate Assignment Committee referred the bill to the Telecommunications and Information Technology

Committee (a good sign) in February, but after two amendments to the bill, the Telecommunications and Information Technology Committee referred the bill back to the Assignments Committee in April, where it has sat ever since (considered a bad sign indicating that the bill may very well die in committee).

While we continue to monitor these issues, companies should continue to review their internal policies and procedures, and should implement general best practices discussed in our previous article — such as arbitration and class action waiver agreements — to deter and, hopefully, avoid being dragged into the current sea of uncertainty.