KILPATRICK
TOWNSEND

February 12, 2019

Keep Your Eye on Biometrics: Illinois High Court Waves Six Flags at Spokeo

by Vita E. Zeltser , John M. Brigagliano , Amanda M. Witt , Jon Neiditz , Ronald L. Raider

Attention all who collect fingerprints and other biometric information of Illinois residents: a private right of action is now available for a mere technical violation of the Illinois Biometric Information Privacy Act (“BIPA”). This development greatly augments an existing liability risk that is significant if a company collects biometric information, since BIPA's statutory damages provision specifies per-violation damages of $1,000 for negligent violations and $5,000 for intentional or reckless violations, or actual damages, if they are greater than those amounts, attorneys’ fees and costs, and injunctive relief. Affected companies include those that collect biometric information about their workforce or customers, and vendors that collect such information about the workforce or customers of their customer companies.

The Decision: No Day At the Amusement Park for Six Flags

On January 20, 2019, the Illinois Supreme Court opened the BIPA class action floodgates a bit wider and breathed new life into the 2008 law in its *Rosenbach v. Six Flags & Great America* decision, by holding that a plaintiff who gave his thumbprint to Six Flags in connection with his purchase of a Six Flags season pass is entitled to seek liquidated damages and injunctive relief pursuant to BIPA. When collecting his thumbprint, the amusement park did not provide the plaintiff with a statutorily required notice, and did not obtain his signed release, amounting to a technical violation of BIPA. The court determined that this technical violation is sufficient to pursue a valid cause of action under BIPA, even in the absence of actual injury or adverse effect beyond a violation of the plaintiff’s statutory rights. The court reasoned that BIPA “vests in individuals and customers the right to control their biometric information by requiring notice before collection and giving them the power to say no by withholding consent.” In reaching its decision, the court relied on the reasoning underpinning BIPA, that a violation of the statute necessarily harms a plaintiff’s right to control his or her biometric information, which is a unique type of data since, unlike any other personal identifier, a biometric identifier cannot be changed or replaced if hacked or stolen.

Leaving Fingerprints on Spokeo?

Requirements for recovery under BIPA in Illinois state courts now contrast sharply with the requirements for such recovery in federal court since procedural, statutory violations of BIPA alone do not constitute the "concrete and particularized injury" currently required by *Spokeo v. Robins* for Article III standing, which is a threshold requirement for a lawsuit to proceed in federal court. For now, expect forum shopping between state and federal court in BIPA actions. Plaintiffs will file actions in Illinois state courts while defendants will want those actions removed to federal court. Stay tuned for additional developments in this area, since all of the critical pieces are in motion: (1) the federal courts have ruled differently on the harms associated with different types of biometrics and different information processes associated with those biometrics, (2) the Illinois Legislature is considering amendments to BIPA that include findings concerning harm, (3) the U.S. Supreme Court is considering cases that may impact the current disparate treatment of Spokeo by different federal courts, (4) state courts may allow litigation to proceed without a demonstration of a Spokeo injury, and, of course, (5) technology marches on.

A Quick Scan of BIPA Requirements

BIPA requires businesses that collect or otherwise obtain retina or iris scans, fingerprints, voiceprints, or scans of hand or face geometry, or any information based on any of the above that is used to identify an individual, to implement protective policies, and provide notices to and obtain releases from such individuals. More specifically, BIPA's substantive provisions include the following:

- **Written Release and Disclosure**. Companies collecting biometric information must obtain a written release from the individual whose data is being collected; the release must discloses the specific purpose and length of time for which the biometric information is being collected, stored, and used.
- **Prohibition on Sale and Disclosure**. Companies that are "in possession" of biometric information are prohibited from (i) selling, leasing, trading, or otherwise profiting from such information; and (ii) otherwise disclosing or disseminating such information unless the individual whose information is at issue consents.
- **Protection**. Companies possessing biometric information must protect such information with at least the same level of protection as that with which the company stores, transmits, and protects other confidential and sensitive information.
- **Destruction**. Companies must have a publically available retention and destruction policy that requires the destruction of biometric information whenever the initial purpose for its collection has been satisfied, or within three years of the individual's last interaction with the company, whichever occurs first.

Other States Recognize Biometrics as a New Face of Privacy

When it was passed in 2008, BIPA was the first law of its kind in the United States. Texas followed Illinois with its own law shortly thereafter and Washington passed a law in 2017. Of the three states with biometric information laws, only Illinois' BIPA provides for a private right of action. In 2019, other states are poised to follow Illinois with Massachusetts and New York proposing BIPA-inspired laws. Laws similar to BIPA have been pending in state legislatures in Delaware, Alaska and Michigan as far back as 2017. Given that there are no federal laws on this issue yet, it is important to monitor state legislatures for additional laws regulating the use and collection of biometric information.