Illinois Supreme Court clarifies standing under biometrics law: No actual harm needed

January 30, 2019

On January 25 2019, the Illinois Supreme Court issued its long-awaited decision in *Rosenbach v. Six Flags* and clarified that no actual harm is needed to have standing to assert a claim under the state's unique Biometric Information Privacy Act (BIPA) (740 ILCS 141 *et seq.*). Enacted in 2008, BIPA governs how private businesses collect, retain, disclose and destroy the biometric information and biometric identifiers of Illinois residents. The law also allows any person "aggrieved" by a violation of its provisions to "have a right of action against an offending party" and to "recover for each violation" the greater of liquidated damages ($1,000 for a violation or $5,000 for an intentional or reckless violation) or actual damages, as well as reasonable attorney fees and costs, and any other relief, including an injunction, the court deems appropriate.

At issue in *Rosenbach* was whether an individual is considered "aggrieved" under BIPA if the individual has not suffered actual harm and only alleges a statutory violation. The Illinois Supreme Court answered the question in the affirmative. The case arose out of a 2014 visit to a Six Flags amusement park by 14-year-old Alexander Rosenbach, the son of plaintiff Stacy Rosenbach. Alexander provided his fingerprint to gain access to the park. Neither mother nor son were informed in writing of the specific purpose and length of term for which the son's fingerprint had been collected. Neither signed a written release regarding the taking of the fingerprint. And neither consented in writing to the collection, storage or use of the fingerprint. BIPA imposes various obligations on covered entities regarding the collection, retention, disclosure and destruction of biometric identifiers and biometric information, including fingerprints, such as an obligation to provide notice to the individual (or individual's representative) and to obtain a written release relating to the storage and use of the biometric information.

Stacy Rosenbach, acting in her capacity as Alexander's mother, brought a class action under BIPA in Lake County, IL, alleging violations of the statute's notice and release provisions. Rosenbach did not allege any actual harm resulting from the alleged violations. The defendants moved to dismiss, in part, on the ground that plaintiff had suffered no actual or threatened injury and therefore lacked standing to sue. The circuit court denied the motion, and the court of appeal reversed, holding that a plaintiff is not an "aggrieved" person under BIPA based solely on a statutory violation without asserting additional injury. Rosenbach appealed, and the state's high court reversed.

According to the Illinois Supreme Court, requiring individuals to plead and prove actual harm before they are entitled to seek redress under BIPA is antithetical to the legislature's purpose in enacting the statute, which was to prevent and deter biometric data from being compromised. The Court also found that sustaining actual damages is not necessary to qualify as "aggrieved" according to the plain meaning of that word, and pointed to parallel language in other statutory regimes where no actual harm is required to have standing.

This decision will likely open the floodgates on additional BIPA litigation. Hundreds of cases that were stayed pending the outcome of *Rosenbach* will now move forward. And privacy advocacy groups are already hailing the decision as an important milestone in the use of BIPA to hold industry accountable. (Of course it doesn't hurt that attorneys' fees are included under the statute.) Whether the decision resolves all questions of standing under BIPA remains to be

seen. Challenges under the statute concerning the definitions of “biometric information” and “biometric identifier” remain. And several standing-related challenges in federal court under Article III remain potentially unaffected by this state court decision.

Takeaways

The decision did not come as a surprise. Based on the questions raised by some of the judges during oral argument last year, and a similar ruling by a California federal judge in March, it was likely the Illinois Supreme Court would come down the way it did. What the Court’s decision makes clear, however, is that BIPA litigation is here to stay and that covered entities should take steps to ensure compliance now. In practical terms, this means that any business collecting any type of biometric information or biometric identifier on an Illinois resident should examine and review its: (1) written external and internal facing policies concerning the collection and treatment of biometric information and biometric identifiers; (2) notice and consent policies and procedures; and (3) cybersecurity policies and procedures.

- Written external and internal facing policies. BIPA requires covered entities to develop a "written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first." 740 ILCS 14/15(a). Covered entities should review their external-facing policies, create new ones if needed, and ensure that any internal-facing policies are adequately aligned to meet this strict statutory requirement.

- Notice requirements. BIPA prohibits covered entities from collecting or using biometric information unless it first: (1) informs the data subject in writing of the collection or use; (2) informs the data subject of the purpose and length for which the collection and use would occur; and (3) obtains a written consent for the same. Covered entities should therefore ensure these written notices and consent mechanisms are in place, and are being properly utilized across all platforms.

- Storage/Protection requirements. BIPA requires covered entities to store, transmit and protect all biometric information and biometric identifiers using the “reasonable standard of care within the private entity’s industry” and to store biometric information and biometric identifiers the same as it protects other sensitive information (i.e., personal information that can be used to uniquely identify an individual, individual’s account or individual’s property). Covered entities should therefore review their information security program (i.e., cybersecurity practices) to ensure they are storing and using biometric information and biometric identifiers in a way that is safe and secure. This is especially true for those entities operating in critical infrastructure, such as healthcare, telecommunications, and oil and gas, because each of these industries has particular cybersecurity frameworks that should be counseled to make sure that biometric information and biometric identifiers are being stored and used in a reasonable manner, as appropriate to the particular entity’s industry. Additionally, entities should ensure they are not treating or storing biometric information or biometric identifiers in a way that is different from other personal information (however defined by the entity).

A final takeaway concerns the interplay between BIPA and California’s new Consumer Privacy Act of 2018 (CCPA), which also governs the collection and use of biometric information, and overlaps in part with BIPA. However, the CCPA does not go into effect until January 1, 2020, so whether and to what extent these statutory regimes overlap, creating potentially conflicting compliance obligations, remains to be seen.

The Dentons Litigation, Privacy and Cybersecurity teams will continue to monitor the BIPA litigation trends, its overlap

with other regulatory and statutory regimes, and stand ready to help you and your business ensure BIPA compliance to mitigate against risk associated with the likely increase in focus under the law.

Your Key Contacts

Kristen C Rodriguez
Partner, Chicago
D +1 312 876 6133
M +1 312 391 8343
kristen.rodriguez@dentons.com

Natalie J. Spears
Partner, Chicago
D +1 312 876 2556
M +1 312 371 8520
natalie.spears@dentons.com

Peter Stockburger
Partner, San Diego
D +1 619 595 8018
peter.stockburger@dentons.com