Just two months after an Illinois appellate court dismissed a similar complaint alleging a violation of the Illinois Biometric Information Privacy Act (BIPA), a California federal court found that a claim asserted under BIPA for an alleged violation of a right to privacy—even without any independent injury or concrete harm—was sufficient to confer Article III standing. BIPA has already given rise to dozens of class action lawsuits against companies that collect, store, or use the biometric information of their customers, employees, or even unwitting individuals. The California decision in *In re: Facebook Biometric Info. Priv. Litig.* increases the risks to companies that use biometric information, particularly in that district, and reinforces the need to strictly comply with the requirements of BIPA and other biometric protection statutes.

Biometric data is information used to identify an individual using that person’s unique biological characteristics. The data is collected using technology such as fingerprint or retina scans or facial recognition software. Government agencies and private companies have collected and used biometric data for a number of purposes, like enhancing security, tracking employees, serving as a substitute for paper or electronic tickets, or even creating “virtual” characters on a video game using the physical characteristics of a human player. Only the risks attendant with its collection and storage outnumber the uses for biometric data: unlike a credit card number, if a thief steals a person’s fingerprint, the owner of the print cannot simply alter it to avoid future identity theft. The tail on the risk may be as long as that person’s life (and even beyond).

BIPA was explicitly enacted to protect the biometric information of Illinois residents by regulating the collection, use, storage, and distribution of such data. Companies must obtain consent from individuals before they obtain biometric information or use it for any purpose.

Enacted in 2008, BIPA is the oldest and most punitive of the biometric protection statutes in the United States. It remains the only biometrics law on the books (for now) that provides for a private right of action, statutory damages, and attorneys’ fees. It is therefore no surprise that over the last year, plaintiffs’ lawyers have filed dozens of putative class actions alleging violations of BIPA, against companies of all sizes, including corporate behemoths like Facebook. More and more states are expected to enact similar biometric protection laws. In the meantime, the recent decision in *In re: Facebook* will provide plenty of headaches for companies that use Illinois residents’ biometric data.

*In re: Facebook* is an amalgam of three separate putative class actions filed against Facebook in Illinois state and federal courts arising from alleged violations of BIPA. The cases were transferred to the Northern District of California and consolidated at the request of the parties. The plaintiffs allege that Facebook did not provide them notice or obtain their consent before collecting data.
their biometric data in the form of their likenesses, in connection with Facebook’s “tagging” feature on photographs.

Most significantly, the plaintiffs did not allege that they suffered any independent injury or concrete harm as a result of the BIPA violations, but the court nevertheless afforded them Article III standing since they held that the Illinois legislature had “codified a right of privacy in personal biometric information.” The court pointed to the language of BIPA, which focused on protecting the right of individuals to protect their unique—and inherent—personally identifiable information and concluded that violation of that right “is quintessentially an intangible harm that constitutes a concrete injury in fact.”

In re: Facebook is significant for two other reasons. First, the court noted that “BIPA expressly recognizes that social security numbers do not implicate the kinds of privacy concerns that biometric identifiers do.” In so holding, the court distinguished biometric suits from the hundreds of data breach class actions filed every year that allege impending threat of future harm based on exposed social security numbers. Second, the court distinguished the allegations in this case from some other notable BIPA decisions because in this case the plaintiffs did not know their data was being collected, and therefore did not implicitly consent to its collection by virtue of their use of Facebook’s services.

This decision stands in contrast with the Illinois appellate court’s dismissal in Rosenbach v. Six Flags, where the court found that the plaintiff was not “aggrieved” under BIPA because he had suffered no injury other than the alleged procedural violation. The Northern District of California has thus provided plaintiffs’ attorneys with a roadmap—at least in cases in that district—to withstand a standing challenge.

While companies that collect, store, and use biometric data should be concerned by the In re: Facebook decision, there are ways to mitigate, or even avoid, liability. A strong compliance program surrounding biometrics, with a focus on obtaining customer or employee consent, is essential. This is even true for companies that do not conduct business or have contacts with Illinois. Although these suits are overwhelmingly filed in Illinois, they are certainly not limited to Illinois defendants, or even plaintiffs. It is also true that while BIPA is the first law of its kind, it is not the only one, and certainly will not be the last, as the use of biometric data becomes more prevalent.

If you have any questions about this legal alert, please feel free to contact any of the attorneys listed under ‘Related People/Contributors’ or the Eversheds Sutherland attorney with whom you regularly work.