BIPA: The Ongoing Threat of Employee Class Actions and Recent Developments

Amundsen Davis Data Privacy & Security Alert
October 9, 2020

Even in the pandemic, the (high) number of class action filings based upon the Illinois Biometric Privacy Act (BIPA) remains steady. And, against that backdrop come two recent decisions that may impact how employers need to shift their defense strategies.

First, in *McDonald v. Symphony Bronzeville Park LLC*, the Illinois Court of Appeals ruled that the state Workers' Compensation Act (WCA) and its exclusivity provisions do not bar claims for statutory damages under BIPA. The court distinguished the two, noting that while the WCA provides remedies to workers that have sustained an actual injury, BIPA provides statutory, liquidated damages to employees who allege privacy right violations even when there is no injury. This outcome should come as no surprise given past rulings on what an employee or consumer needs to show to pursue a BIPA claim. Thus, as it relates to BIPA claims, the WCA exclusivity defense is no longer viable – or at least for the time being, since this case will likely be appealed to the Illinois Supreme Court.

In a second decision, *Williams v. Jackson Park SLF, LLC*, the Northern District of Illinois held that union workers under a collective bargaining agreement are preempted from pursuing a BIPA cause of action in federal court. The overall success of this argument, though, may be limited as the court is allowing the plaintiff to amend its complaint, meaning the case may still be litigated by non-union class members. It remains to be seen what defenses to the merits—and perhaps, more importantly, to class certification—can be advanced with an amended complaint and amended class definition.

On balance: it has been 12 years since BIPA was enacted, but there are still so many questions that are being battled in court as employers and employees continue to navigate this biometric privacy law. One thing is for certain: BIPA packs a punch with eye-popping statutory damages and monetary awards that can lead to anywhere from $1,000 to $5,000 per violation plus attorneys' fees. Moreover, considering that an *alleged* violation is enough to bring a suit, BIPA is a class action dream – bearing in mind if an employer is collecting biometric data on one individual, it is collecting it on many individuals.

PROFESSIONALS

Molly A. Arranz
Partner

RELATED SERVICES

Biometric Privacy

Class Action

Cybersecurity & Data Privacy

Employment Advice & Counsel

Labor, Employment & Immigration

To avoid finding yourself facing a BIPA class action, the best thing you can do as an employer is ensure basic compliance in the first place:

- **Determine what biometric information you are collecting.** Under BIPA, biometric data is sensitive information that is biologically unique—such as iris scans, fingerprints, voiceprints, and face geometry. Both of the recent lawsuits were brought by employees using finger prints or hand prints to clock in and out of work. While these may now seem like obvious identifiers, remember that some identifiers can be captured simply through voice or video recording. That being said, while advanced technology can enhance the workplace experience, when integrating new systems think through what information your company may be collecting in order to determine any necessary disclosures.
- **Evaluate what disclosures you currently have in place.** To comply with BIPA, companies must provide written notice to its users disclaiming what biometric information will be collected, stored, or used, as well as an explanation of the purpose of its collection. Additionally, prior to collection it is best to obtain *express written authorization* from employees to collect and store their biometric information.
- **Create a public facing policy that is easily accessible for employees.** Biometric data has become a hot button issue across the country. Since biometric information is uniquely sensitive and cannot be changed, there is constant, growing concern on how information is being collected, stored, and destroyed. Creating a company policy that is available to employees is not only required, but helps ease some concern. Consider posting the policy in public spaces like breakrooms, or perhaps in areas where the biometric data is being used. For example, if your employees clock in via fingerprints, then perhaps it is worth posting a copy of the policy near the time clock.
- **Stay alert to both recent court decisions and pending regulations.** BIPA has caused quite a stir and will continue to be challenged in courts as employers and employees alike learn what can and cannot be brought under BIPA. While staying up to date on recent court decisions is always beneficial, it is also important to be alert to any regulatory changes so that your business can remain in compliance. Recently, the National Biometric Information Act of 2020 was introduced in the U.S. Senate. If passed, this would be the first comprehensive federal policy of its kind concerning biometric data. Since this bill has only been introduced you are not subject to any official requirements as of yet. However, the more you are aware of upcoming regulations, the better prepared your company will be with efficiently and effectively complying.

Want to learn more about BIPA and how you can avoid the threat of a class action? Join Molly Arranz and Carlos Arévalo for a complimentary webcast on October 29.