Employer Beware: Proposed Biometric Information Regulation May Impact Florida Employers

By: Natasha T. Khoyi[i] *and* Edward B. Carlstedt, FordHarrison LLP

As with any proposed legislation, employers must beware of the legal pitfalls that lie in wait for them, surprising those who have not considered the creative lawsuits plaintiffs' attorneys may conjure. The most recent proposed legislation to note in Florida is the "Florida Biometric Information Privacy Act" (FBIPA)[1], which would govern an employer's use of biometric technology. On February 21, 2019, the Florida Legislature introduced the FBIPA, which is designed to regulate private entities' use, collection, and maintenance of biometric identifiers and biometric information. If the proposed bill is passed, the FBIPA would create a private right of action against employers that misuse or improperly maintain or collect biometric information. This could lead to increased litigation against employers, as Illinois' employers have experienced, where similar legislation is already in place. Plaintiffs in such cases argue that they were not properly advised of the use of their biometric information, and would never have agreed to it without additional compensation under a theory that their employment agreement was altered without the employer providing new or additional consideration. Of course, these lawsuits are not limited to just employer-employee relationships, and consumers are suing under similar lack of notice/consideration theories.

Biometric technology refers to technology used to authenticate, store, or otherwise utilize metrics and calculations relating to the human body. Biometric identifiers may include fingerprints, palm prints, facial recognition, or iris or retina recognition. As technology has advanced, employers have increasingly used employee biometric information, such as fingerprints, to track work hours and for customer access control. Facial recognition has been used for social media tracking and other access control measures. While these advancements have helped create more effective security systems, decreasing the costs of devastating security breaches in the long term, the newly proposed FBIPA could create a new point of attack against businesses—litigation brought by employees and customers whose information has allegedly been improperly collected, used, disseminated or maintained by the business.

Notably, the proposed form of the FBIPA is almost identical to the Illinois Biometric Privacy Act (IBIPA), which was enacted in 2008. Since then, other states, including Washington and Texas, have followed Illinois' lead, enacting or proposing their own form of legislation to govern the collection, use, and storage of biometric information. However, the prevalence of laws governing biometric information and its use has led to a slew of lawsuits, including over 200 cases against private companies in Illinois alone since the enactment of the IBIPA. Several of these lawsuits have taken the form of class actions

[1] Florida Biometric Information Protection Act has been proposed as HB 1153, a bill from House Representative Bobby Dubose, and as SB 1270, a bill from Senator Gary Farmer, Jr., which are identical to one another.

seeking damages for employers' alleged misuse of employee fingerprints and facial recognition technology.

On its face, the onslaught of litigation may seem appropriate where employers have misused employee biometric information; however, one of the most alarming issues Illinois employers have faced is the Illinois Supreme Court's ruling in *Rosenbach v. Six Flags Entertainment Corp.* that an employee need not suffer damages to recover for violations of the IBIPA. Cases brought under the IBIPA increased exponentially after the court's January 2019 ruling in *Rosenbach.* However, claims by employees that are not supported by actual damages could be subject to standing challenges in federal court, which could stem the tide of litigation somewhat.

In *Liu v. Four Seasons Hotel Ltd.*, the First District Court in Illinois found that an arbitration agreement must specifically include biometric privacy claims to permit those to be arbitrated. However, preemption in accordance with collective bargaining agreements has been raised as a defense and, pending the decision in *De La Rosa v. Choice Hotels International, Inc.*, could be an option for employers.

As proposed, the FBIPA would require private entities to develop a publicly available written policy establishing a retention schedule and guidelines for destroying biometric information upon satisfaction of the initial purpose for collecting the information or within three years after the individual's last interaction with the private entity, whichever occurs first. Additionally, before collecting the information, the entity would be required to obtain a written release executed by the individual supplying the biometric information and inform the individual of the purpose for obtaining the biometric information and the length of time that it will be collected, stored, and used. Furthermore, private entities would be prohibited from disclosing biometric information unless: the individual who supplied the biometric information consents to such disclosure; the disclosure completes a financial transaction authorized by the individual; the disclosure is required by law; or the disclosure is required pursuant to a warrant or subpoena. To protect biometric information, a private entity must store and transmit the information using the reasonable standard of care within that entity's industry and do so in a manner that is the same as or more protective than the manner in which it stores, transmits, and protects other confidential and sensitive information.

Hopefully the Florida Legislature will take care to craft the final form of the FBIPA so that it effectively describes prohibited activities in a manner that enables pragmatic and continued use of technological advancements. In the meantime, Florida employers must be mindful of the proposed form of the FBIPA and begin taking action now to prevent future litigation as seen by so many Illinois employers. Specifically, Florida employers should consider adding biometric privacy claims to their arbitration agreements to avoid a finding disallowing arbitration. Additionally, employers should consider modifying employment agreements to include a description of permissible uses of biometric information. Employers should pay close attention to the scope of biometric information uses as technology advances and should update agreements accordingly, sending appropriate riders and/or notices to current employees. By analyzing and assessing these

issues now, prior to the passing of the FBIPA, employers can remain ahead of the plaintiffs' bar, which is undoubtedly waiting to pounce if and when a private right of action is instituted through the FBIPA.

Looking ahead, it is likely there will be a significant influx of lawsuits brought if the FBIPA is enacted as proposed, with a private right of action similar to that found in the IBIPA. All private entities should consider examining their use of biometric information and assessing whether changes are necessary or new agreements need to be put in place.

---

[i] If you have any questions regarding this article, please feel free to contact the authors, Natasha Khoyi, 813-261-7823, nkhoyi@fordharrison.com, or Ed Carlstedt, 813-261-7895, ecarlstedt@fordharrison.com, or the FordHarrison attorney with whom you usually work.