THE
NATIONAL LAW REVIEW

Biometric Privacy Update – Actual Harm Not Required

Thursday, February 7, 2019

Since the passage of the Illinois Biometric Information Privacy Act (BIPA) in 2008, it has been used by plaintiffs' attorneys to sue companies that use biometric identification technologies. Many BIPA cases have failed because courts routinely dismissed such actions for failing to allege proof of actual damages or actual injury. A recent decision of the Illinois Supreme Court changed the landscape of pending and future actions when it held that a mere technical violation of BIPA was sufficient to establish that a person was "aggrieved" such that he/she can recover statutory damages under the Act.

Article By Michael W. Weaver
Ryan S. Higgins Lynette Ryan Arce
Daniel Campbell Matthew R. Cin
Austin Mooney McDermott Will & Emery
On the Subject Communications, Media & Internet
Labor & Employment
Litigation / Trial Practice
Illinois

IN DEPTH

A recent decision by the Illinois Supreme Court raises the stakes for organizations that are required to comply with the Illinois Biometric Information Privacy Act (the Act or BIPA).

On January 25, 2019, in *Rosenbach v. Six Flags Entertainment Corporation et al.*, the Illinois Supreme Court held that a plaintiff need not demonstrate actual injury or harm in order to be awarded monetary damages under BIPA. Broadly summarized, BIPA vests in individuals the right to control their biometric information by requiring notice to the individual before an organization collects the information and by giving the individual an opportunity to object by withholding consent to that collection. The Illinois Supreme Court held that failure to adhere to these procedures is not just a "technical" violation of BIPA but rather results in "the right of the individual to maintain [his or] her biometric privacy vanish[ing] into thin air," which is a "real and significant" injury and the "precise harm the Illinois legislature sought to prevent" with BIPA.

This decision underscores the need for organizations implementing biometric technologies, particularly in Illinois, to maintain robust programs for compliance with the developing set of laws regulating the collection and processing of biometric information.

The Regulatory Landscape

Biometric identification technologies are increasingly prevalent in daily life. Employees may encounter them for timekeeping purposes, consumers may use them to pay at grocery stores and gas stations, and air travelers may encounter them at security checkpoints. While biometric identification technologies offer obvious benefits to individuals in terms of convenience, there are countervailing privacy and security considerations, and state legislatures are responding.

Illinois became the first state to regulate the collection, use, safeguarding, handling, storage, retention and destruction of biometric data (*e.g.*, retina or iris scan, fingerprint, voiceprint, or hand- or face-geometry scan) with the enactment of BIPA in 2008. The Illinois legislature recognized the unique privacy and security considerations around biometric identifiers in its legislative findings.

> Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no

recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.

BIPA requires organizations to, among other things (i) inform an individual in writing of the biometric data collected and the purpose and length of time for which the company will collect, store and use such data, and (ii) receive a written release prior to taking or retaining his or her biometric information.

While other states have adopted similar statutory protections (Texas and Washington) and yet others have considered them (Alaska, Connecticut, Montana, and New Hampshire), Illinois is the only state that has provided individuals with a private right of action to obtain damages for violations of the Act.

The full weight of BIPA's impact did not occur until several years after its enactment when numerous class action complaints were filed, primarily by employees against employers for violating the notice and consent provisions of the Act. Over the last few years, we have seen a surge in biometric privacy lawsuits in Illinois. Illinois circuit courts have presided over at least 100 BIPA cases in the last two years, particularly because BIPA provides for a private right of action for violations. The cost of non-compliance can be substantial. In the case of negligent violations, private entities are liable for $1,000 per violation in liquidated damages or the amount of actual damages, whichever is greater. For intentional or reckless violations, liquidated damages increase to $5,000 per violation or actual damages. Private entities are also liable for reasonable attorneys' fees, costs, experts' fees, and injunctive relief.

BIPA expressly provides that "any person aggrieved by a violation" of the Act may pursue money damages and injunctive relief against the offending party, however, the Act does not define the term "aggrieved" or "person aggrieved." The issue addressed by the Illinois Supreme Court was whether a plaintiff who alleged only a "technical" violation of the Act without alleging some actual injury or damage is an aggrieved person. Defendants most often, and most successfully, cited to the US Supreme Court's decision in *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016), which holds that "a bare procedural violation, divorced from any concrete harm," fails to satisfy the injury-in-fact requirement to show "standing" to sue under Article III of the US Constitution. *Id.* at 1549. While Article III does not constrain state courts, the *Spokeo* arguments proffered by defendants in federal cases inspired the arguments made by defendants in BIPA cases—that violations of BIPA were merely technical violations of a statute that do not "aggrieve" a person because the injury does not result in actual harm. In *Rosenbach v. Six Flags Corporation*, the Illinois Supreme Court rejected these arguments regarding the definition of "aggrieved" in BIPA.

Rosenbach v. Six Flags Corporation

The Illinois Appellate Court entered the fray as to the meaning of "aggrieved" through two opinions: *Rosenbach v. Six Flags Entertainment Corp.*, 2017 IL App (2d) 170317 and *Sekura v. Krishna Schaumburg Tan*, Inc., 2018 IL App (1st) 180175.

The Second District Appellate Court issued the first ruling in *Rosenbach*. The *Rosenbach* plaintiff—a 14-year-old boy—asserted a violation of BIPA after he purchased a season pass for a Great America theme park. At the time he registered, defendants obtained his fingerprints, but defendants allegedly failed to obtain his written consent or disclosed its plan for the collection, storage, use or destruction of the biometric information, both of which are required by BIPA. Plaintiff did not allege any actual injury, but simply alleged that if plaintiff was fully aware of defendants' conduct, the boy would have never purchased the pass. The trial court denied defendants' motion to dismiss but certified two questions to the Appellate Court on the meaning of "aggrieved" person under the Act.

In answering these questions, the Second District analyzed how "aggrieved" person was viewed in other legal contexts, *i.e.*, by a federal district court dealing with BIPA, the Wisconsin Appellate Court, and the Hawaii Supreme Court, all of which equated "aggrieved" with an actual injury. *Rosenbach*, 2017 IL App (2d) 170317, ¶ 22; *see McCollough v. Smarte Carte, Inc.*, No. 16-C-03777, 2016 WL 4077108 (N.D. Ill. Aug. 1, 2016); *Avudria v. McGlone Mortgage Co.*, 2011 WI App 95, 802 N.W.2d 524 (2011); *AlohaCare v. Ito*, 271 P.3d 621 (Haw. 2012). The Second District found that a private right of action for a "technical" violation of the statute, *i.e.*, a violation that did not cause actual harm, would render the word "aggrieved" superfluous in the Act. *Id.* at ¶ 23. As a result, the Second District found that in order to maintain a private right of action, a "person aggrieved" must allege some actual harm.

Ten months later, the First District Appellate Court reached the opposite conclusion in *Sekura*. Here, a customer of L.A. Tan provided her fingerprint when she purchased membership at the tanning salon. *Sekura*, 2018 IL App (1st) 180175, ¶ 8. The First District analyzed the plain language of BIPA noting that the Act "does *not* state a person aggrieved by a violation of this Act—plus some additional harm—may sue." *Id.* at ¶ 50 (emphasis in original). Instead, the legislature chose to state only a "violation of this Act" gives rise to a private right of action. *Id.* These two decisions caused a serious fissure in Illinois law as one required actual harm to sue under BIPA and the other did not. Both decisions were appealed to the Illinois Supreme Court.

The Illinois Supreme Court resolved this split through its unanimous opinion in *Rosenbach*, 2019 IL 123186, by reversing the Second District decision in *Rosenbach* and implicitly affirming the First District in *Sekura*. The court reviewed various Illinois statutory provisions which provided individuals a private right of action and divided them into two categories: those that imposed a requirement of actual harm, *e.g.*, Section 10(a) of the Consumer Fraud and Deceptive Business Practices Act, and those that do not, *e.g.*, the AIDS Confidentiality Act. *Id.* at ¶¶ 25, 26. Based on the statutory language, the court viewed BIPA as falling to the latter category in not requiring an actual injury. Further, the court, going back to precedence from 1913, noted that the term "aggrieved" as defined under the law does not require one to be actually harmed. *Id.* at ¶¶ 30, 31.

Finally, the court rejected the very concept of a "technical" violation of the Act. The court noted that the Act "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." *Id.* at ¶ 34. The court continued that "[t]hese procedural protections are particularly crucial in our digital world because technology now permits the wholesale collection and storage or an individual's unique biometric identifiers—identifiers that cannot be changed if compromised or misused." *Id. quoting Patel v. Facebook Inc.*, 290 F. Supp. 3d 948, 954 (N.D. Cal. 2018). When this biometric information is risked—through the failure to adhere to the statutory requirements set forth in the Act—the court found that it is "no mere technicality" and "[t]he injury is real and significant," which allows for a private right of action as designed by the legislature. *Id.* at ¶ 34. By rejecting the very concept of a "technical" violation of the Act, the Illinois Supreme Court impliedly rejected arguments based on US Supreme Court's rationale in *Spokeo*, discussed above. Indeed, *Spokeo* is not mentioned in the Illinois Supreme Court decision at all. This is notable because several *amicus* briefs cited the parallels between the rationale in *Spokeo* and how that rationale is consistent with Illinois precedent. In ignoring the *Spokeo* rationale, the *Rosenbach* decision highlights the different approaches to injury between state courts, which do not have to meet the high bar of Article III standing, and federal courts, which do.

Significance of *Rosenbach* Decision

Rosenbach will have significant implications for organizations implementing biometric technologies and on the 200+ similar pending cases in Illinois. To avoid litigation, organizations should closely scrutinize their biometric practices to comply with BIPA, including by providing adequate notice sufficient to create an informed, written consent to the collection, use and disclosure of biometric data before such data is collected. Organizations should also limit the scope of their collection and use of biometric information as narrowly as possible so that the minimal amount of biometric information is in the organizations' possession. Organizations should take stock of their current practices involving the collection, use, and storage of biometric information to ensure their policies at least encompass the minimum requirements of the law. The series of lawsuits alleging BIPA violations demonstrates that no infraction is too small to draw ire from a potential plaintiff. Therefore, once an organization has proper policies and notice and consent processes in place, the organization will need to provide detailed training to its employees charged with carrying out the organization's biometric information practices on an annual and as needed basis.

In addition to the steps organizations can take to comply with the BIPA, it is important to involve litigators early in the process when sued for a BIPA violation. There are several strategies that organizations can use to defend against BIPA-related lawsuits. Early involvement of counsel is important as we anticipate that the *Rosenbach* decision will result in hundreds more BIPA actions, many of which we believe will be pursued as class or collective actions, which will dramatically increase the cost of defense and the amounts at issue in the cases.