The CYBERSECURITY LAW REPORT

www.cslawreport.com Vol. 4, No.42 December 12, 2018

IDENTITY MANAGEMENT

Illinois Appellate Decision Creates Split on Standing to Sue Under BIPA

By Vincent Pitaro, *The Cybersecurity Law Report*

The Illinois Biometric Information Privacy Act (BIPA or the Act), a groundbreaking statute that specifies requirements for the collection and handling of biometric data, has been the basis for a number of standing cases. The recent decision by the Appellate Court of Illinois, First District (Court), in Klaudia Sekura v. Krishna Schaumburg Tan, Inc. (Decision), has lowered the bar for plaintiffs, although a pending Illinois Supreme Court decision in a different case may raise it again. This article analyzes the Decision and other relevant cases, with insights from Jackson Lewis principals Jason C. Gavejian and Joseph J. Lazzarotti.

See also "Actions Under Biometric Privacy Laws Highlight Related Risks" (Dec. 6, 2017).

BIPA Requirements

In 2008, Illinois adopted the Biometric Information Privacy Act (BIPA or the Act), which:

- requires an entity to have a written retention and destruction policy pertaining to the biometric data it collects;
- requires the entity to advise the persons from whom it collects that data of the collection, the purpose for doing so, and the time frame for holding the data, and to obtain a written release from those persons;
- prohibits the entity from selling or profiting from that data;
- prohibits the entity from disclosing that data without the person's consent, except for certain specified purposes; and
- requires the entity to use reasonable care in handling that data.

See also "Colorado's Revised Cybersecurity Law Clarifies and Strengthens Existing Requirements," (Sep. 12, 2018).

Alleged BIPA Violations and Circuit Court Decision

According to the Decision, defendant Krishna Schaumburg Tan, Inc. (KS Tan) is a franchisee of L.A. Tan Enterprises, Inc. (LA Tan). KS Tan's customers are required to have their fingerprints scanned in order to gain access to LA Tan locations. LA Tan shares customer fingerprint data with SunLync, an out-of-state third-party vendor. In April 2015, plaintiff Klaudia Sekura purchased a membership with KS Tan and was required to have her fingerprint scanned. She also had to scan her fingerprints each time she visited KS Tan.

For more on biometric identifiers, see "Finding the Best Ways to Secure Digital Transactions in a Mobile World" (Oct. 19, 2016).

Sekura Complaint

In 2016, Sekura became the lead plaintiff in a class action lawsuit against KS Tan that was filed in Cook County Circuit Court (Circuit Court). Her three-count complaint alleged violation of BIPA, unjust enrichment and negligence. Sekura claimed that KS Tan had violated BIPA in the following ways:

- KS Tan collected, used, stored and disclosed Sekura's biometric data without obtaining a written release from her.
- It disclosed her biometric data to SunLync.
- It never informed her of the specific purpose for collecting her fingerprint data or the length of time that it would use that data.
- It did not provide a publicly-available biometric data retention policy or guidelines for permanently deleting that biometric data.

Sekura further alleged that many LA Tan salons had been in foreclosure in 2013 and that customers had not been told what would happen to their biometric data if those salons went out of business. She also alleged that "she becomes emotionally upset and suffers from mental anguish when she thinks about what would happen to her biometric data if defendant went bankrupt or out of business or if defendant's franchisor, L.A. Tan, went bankrupt or out of business, or if defendant shares her biometric data with others."

Biometric data is commonly covered under state data breach notification laws. See "Analyzing New and Amended State Breach Notification Laws" (Jun. 6, 2018).

Prior Proceedings

In February 2017, the Circuit Court granted KS Tan's motion to dismiss the unjust enrichment count of Sekura's complaint, but denied its motion to dismiss the BIPA claim.

©2018 The Cybersecurity Law Report. All rights reserved.

The CYBERSECURITY LAW REPORT

www.cslawreport.com Vol. 4, No.42 December 12, 2018

In December 2017, in Rosenbach v. Six Flags Entertainment Corp., the Appellate Court of Illinois, Second District, ruled that in order to have standing to sue under BIPA, in addition to an alleged violation of the Act, a plaintiff had to have alleged she suffered an "injury or adverse effect." Like Sekura, plaintiff Rosenbach claimed that the defendant had fingerprinted customers "without obtaining any consent or disclosing its plan for the collection, storage, use or destruction of its customers' biometric identifiers." Six Flags moved to dismiss the case on the ground that plaintiff lacked standing to sue because she had not alleged any injury. The Appellate Court's decision is being appealed to the Illinois Supreme Court.

In light of the Rosenbach decision, KS Tan asked the Circuit Court to reconsider its motion to dismiss Sekura's BIPA claim. In January 2018, the Circuit Court, relying on Rosenbach, reversed its prior ruling and dismissed Sekura's BIPA claim with prejudice.

Sekura appealed that dismissal. For the reasons discussed below, the Court declined to follow Rosenbach and reversed the Circuit Court's decision. The Court concluded that Sekura was entitled to sue solely on the basis of KS Tan's alleged violation of BIPA. Moreover, even if Rosenbach had been correctly decided, the Court stated that Sekura's allegations of emotional distress and violation of her privacy rights were sufficient to satisfy Rosenbach's requirement that a plaintiff allege an injury or adverse effect beyond mere violation of BIPA.

See also "Biometric Data Protection Laws and Litigation Strategies (Part One of Two)" (Jan. 31, 2018); Part Two (Feb. 14, 2018).

Appellate Court Finds Standing to Sue

The sole issue on appeal was "whether a harm or injury, in addition to the violation of the Act itself, is required in order to have standing to sue under the Act." The Court's ruling turned largely on the meaning of the word "aggrieved" in Section 20 of BIPA, which provides, in relevant part: "Any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party." In concluding that a plaintiff is not required to allege any harm beyond a violation of the Act in order to have standing to sue, the Court relied on long-standing principles of statutory interpretation.

Plain Language

The Court concluded that the plain language of Section 20 does not contemplate any harm in addition to "a violation of this Act." Had the legislators intended to require some additional harm, they could easily have said so. This reading is also supported by the fact that Section 20 provides for both liquidated and actual damages. A plaintiff is not required to prove actual damages in order to recover, the Court reasoned.

Definition of "Aggrieved"

According to the Decision, Black's Law Dictionary defines "aggrieved" as "having legal rights that are adversely affected." Similarly, one of the definitions of that term on Dictionary.com is "deprived of legal rights." Here, plaintiff Sekura was aggrieved by the violation of her privacy rights under BIPA. The Court rejected KS Tan's argument that the word "aggrieved" was superfluous. Under KS Tan's reading of Section 20, any person could sue for a violation of BIPA, regardless of whether that person's biometric data was the subject of the violation. "[I] t cannot be that any person, who finds a violation of the Act, may sue. Instead, it must be a person whose privacy rights under the Act were 'aggrieved by' the violation," the Court reasoned.

BIPA does not explicitly create a right of privacy to biometric data. The Court infers that right from the fact that BIPA "prohibits private entities from obtaining biometric information without a release," Gavejian and Lazzarotti told The Cybersecurity Law Report. "Where a law erects certain barriers or conditions for the processing of certain sets of personal data, there is support for the recognition of a right of privacy in such data for the subject of that data." As a result, "if a data subject has a right to not have his or her protected data disclosed without consent, disclosing such data without consent violates the subject's legal rights, resulting in the subject being aggrieved. At that point, the subject does not need to show actual damages because the subject is sufficiently aggrieved by the adverse effect on his or her legal rights," they explained.

Legislative History

Even if BIPA were ambiguous, the legislative history of the law supported the Court's conclusion. Legislators recognized the fact that, unlike a password or similar identifier, a person's fingerprint or other biometric data cannot be changed, making loss of that data particularly worrisome.

The Court rejected the defendant's contention that standing should arise only after actual compromise of a person's biometric data: "Waiting until the harm has already occurred is too late because, as the drafters found, once a person's biometric identifiers have been compromised, there is simply 'no recourse' for prevention. . . . Forcing a member of the public to wait until after an irretrievable harm has already occurred

©2018 The Cybersecurity Law Report. All rights reserved.

in order to sue would confound the very purpose of the Act." Moreover, Sekura had alleged that KS Tan had divulged her biometric data to SunLync, a third-party out-of-state vendor. On a motion to dismiss, that allegation was sufficient. Sekura did not have to allege actual use of her data by SunLync.

Finally, the "right of action" provision of the Illinois AIDS Confidentiality Act is "quite similar" to Section 20 of BIPA, the Court noted. It uses the term "aggrieved" in the same way and provides for both liquidated and actual damages. According to the Decision, an Illinois appellate court has ruled unanimously that a person may recover liquidated damages under that law without proof of actual damages.

Rosenbach Distinguished

The Court rejected the reasoning of the Rosenbach court and declined to follow that decision. However, the Court pointed out that, even if Rosenbach had been decided correctly, Sekura would still have standing to sue because she did allege harm in addition to KS Tan's violation of BIPA.

Right to Privacy

First, she alleged disclosure of her biometric data to SunLync violated her "legal right to privacy of her own biometric information." The Court cited the reasoning of an Illinois federal district court in Dixon v. Washington & Jane Smith Community-Beverly. In that case, plaintiff alleged that the defendant had disclosed her fingerprint data to a third-party vendor without her knowledge, thereby violating her "right to privacy in her biometric information" (citation omitted). The district court concluded that plaintiff had alleged "an actual and concrete injury" that distinguished the case from Rosenbach.

Mental Anguish

Second, Sekura alleged "mental anguish" as a result of that disclosure. The Court distinguished the facts of this case from the Seventh Circuit's standing decision in Gubala v. Time Warner Cable, Inc. because, unlike plaintiff Gubala, Sekura alleged that she suffered mental anguish as a result of KS Tan's alleged violation of BIPA.

See "Third and Seventh Circuits Shed New Light on Spokeo Standing Analysis" (Feb. 8, 2017).

Whether cases that rest on a claim of mental anguish will face an uphill battle "will depend on the language in the particular statute, and the jurisdiction," Gavejian and Lazzarotti noted, adding that "claims based solely on mental anguish will always face evidentiary difficulties." The Decision suggests that even if Sekura had not alleged disclosure to a third party, the Court might have ruled that mental anguish constitutes a sufficient injury or adverse effect, they added. It remains to be seen whether pleading of either a violation of a privacy right and/or mental anguish become the exceptions that swallow the rule for plaintiffs suing under BIPA.

Rosenbach Appeal

On November 20, 2018, the Illinois Supreme Court heard oral argument on the Rosenbach appeal. At oral argument, the judges suggested that "the loss of biometric information could create 'dire consequences' for those individuals whose information was lost and allowing for these types of claims may 'give the Act some teeth,'" Gavejian and Lazzarotti noted. At the same time, "the Court did note that the intent of the statute appears to put a burden on entities that collect biometric information to do certain things as opposed to creating this type of legal claim," they added.

A decision on the Rosenbach appeal is pending, which should resolve the issue of standing under BIPA. Companies are hoping that courts will "ultimately conclude that in order for a plaintiff to bring a claim under BIPA, in order for the plaintiff to be considered a 'person aggrieved,' the plaintiff would have to allege actual harm, and not just a procedural or technical violation of the statute," Gavejian and Lazzarotti said.

Practical Implications of Sekura

Rosenbach, Sekura, Dixon and other BIPA cases "all serve as a reminder of the importance in taking steps now to comply with BIPA's requirements to avoid the risk of liability," Gavejian and Lazzarotti cautioned.

Individuals are becoming increasingly aware of the use of big data, AI and similar technologies, and of efforts to collect, analyze and profit from individuals' data, Gavejian and Lazzarotti pointed out. Reports of data breaches are heightening those concerns. They noted that people are asking questions such as, "Why do they need to have (or continue to have) my personal information? Is it being protected? What are they using it for? Can I ask that my personal information be deleted or erased?"

Individuals may also be concerned about what will happen to their data if the collector goes out of business or shares it with a third party. Finally, the principles enunciated under the GDPR are beginning to "seep into U.S. law," as evidenced by the recent introduction of the California Consumer Privacy Act, they noted. "It would not be surprising, therefore, to see

©2018 The Cybersecurity Law Report. All rights reserved.

courts be more open to accept allegations framed [in terms of violations of privacy rights or mental anguish]," they opined.

See "What to Expect From California's Expansive Privacy Legislation" (Jul. 18, 2018); and "Countdown to GDPR Enforcement: Final Steps and Looking Ahead" (May 16, 2018).

To ensure that they are in compliance with BIPA, Gavejian and Lazzarotti advised companies that collect biometric data from Illinois residents to "review their time management, point of purchase, physical security or other systems that obtain, use, or disclose biometric information against the requirements [of BIPA]." And "[i]n the event they find technical or procedural gaps in compliance – such as not providing notice, obtaining a consent to provide biometric information to a third party, or maintaining a policy and guidelines for the retention and destruction of biometric information – they need to quickly remedy those gaps."

Another BIPA Case to Watch

In a similar BIPA action, on October 19, 2018, Christopher Byczek filed a class action complaint against Xanitos, Inc., alleging BIPA violations that are substantially similar to those alleged by Sekura. According to the compliant, Xanitos, which provides services to hospitals, requires all employees to have their fingerprints scanned into its database for timekeeping purposes. Byczek purports to represent all Illinois residents whose fingerprints were scanned by Xanitos while residing in Illinois.

The single cause of action in the complaint closely tracks BIPA. Xanitos allegedly negligently violated BIPA by:

- collecting, storing and using class members' biometric data prior to obtaining written releases;
- failing to inform class members in writing that it was collecting and storing their biometric data;
- failing to inform them in writing of the purpose and length of time for which their biometric data was being collected, stored and used; and
- failing to provide a public retention schedule for the collected biometric data.

In addition, Byczek alleges that "Xanitos violated Plaintiff's and the Class's rights to privacy in their biometric information as set forth in the BIPA. . . ." However, there is no allegation that Xanitos shared its employee fingerprint data with any third party or that the data has been compromised.

Byczek seeks certification of the purported class, a declaration that Xanitos violated BIPA, statutory damages of $1,000 per violation, pre- and post-judgment interest, equitable and injunctive relief, and attorneys' fees and expenses.

For more on class actions and standing, see "Defense and Plaintiff Perspectives on How to Survive Data Privacy Collateral Litigation" (Mar. 8, 2017); "Minimizing Class Action Risk in Breach Response" (Jun. 8, 2016); "Spokeo's Impact on Data Breach Cases: The Class Action Floodgates Have Not Been Opened, But the Door Has Not Been Locked" (May 25, 2016).

©2018 The Cybersecurity Law Report. All rights reserved.