3-4-2020

New Developments of the Illinois Biometric Information Privacy Act ("BIPA")

Zack Perlitsh
Cardozo Arts & Entertainment Law Journal

New Developments of the Illinois Biometric Information Privacy Act ("BIPA")

BY ZACK PERLITSH/ ON MARCH 4, 2020

Image by Gerd Altmann from Pixabay

In recent weeks, an Illinois statute enacted in 2008 has garnered much attention from the legal community. The Illinois Biometric Information Privacy Act ("BIPA") governs the retention, collection, disclosure and destruction of biometric identifiers and biometric information ("biometric data") by private entities.[1]

BIPA requires private entities possessing biometric data to establish a publicly available policy detailing a data retention schedule and guidelines for permanently deleting the data.[2] Under BIPA an entity may only "collect, capture, purchase, receive through trade, or otherwise obtain" an individual's biometric data if they first (1) notify the individual in writing that their biometric data is being collected or stored, (2) notify the individual in writing of the purpose and length of time the biometric data is being "collected, stored, and used," and (3) "receive[] a written release executed by the subject of the" biometric data.[3]

BIPA has made headlines due in large part to the extremely plaintiff friendly structure and judicial interpretation of its enforcement provision. BIPA provides for a private right of action

by any "person aggrieved by a violation" of the Act against willful, negligent and reckless parties.[4] For each individual violation, a plaintiff may recover (1) the greater of liquidated or actual damages, and (2) attorneys' fees and costs.[5]

There are strong policy reasons for enacting a statute that staunchly protects individual's biometric data. The use of biometric data is still in its relatively infantile stage making the full ramifications of biometric technology unknown.[6] Further, the inherent, biologically linked, uniqueness that the biometric data contains warrants its heightened protection.[7] The legislature highlighted the fact that if one's social security number is compromised it can be changed, whereas biometric data is permanent and if compromised the individual is forever at risk.[8]

Rosenbach v. Six Flags, a case decided by the Supreme Court of Illinois in January 2019, hinged on the interpretation of the enforcement provisions of BIPA and whether actual damages need to be alleged in order to bring an action under BIPA.[9] In *Rosenbach* it was alleged that in order for a 14-year-old boy to enter Six Flags and claim his entry pass, he was required to, among other things, provide his fingerprint. The alleged BIPA violations included (1) collecting, capturing, storing, or obtaining biometric data without written notice, (2) lack of notice regarding purpose of collection and length of use, and (3) not obtaining a written release of the biometric data.[10]

The *Rosenbach* court held that an individual may allege a mere violation of their rights under BIPA, without any additional actual damages, to "qualify as an 'aggrieved' person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act."[11] The court held that a mere technical violation of BIPA would be sufficient to maintain an actionable claim.

In August 2019, the 9th Circuit expanded *Rosenbach* to grant Article III standing where it was alleged that BIPA was violated. In *Patel v. Facebook* it was alleged that Facebook subjected a class of plaintiffs to facial recognition-technology (via the "Tag Suggestions" features) without providing notice and without maintaining a retention and destruction schedule as required by BIPA.[12] Facebook extracted geometric data points from users photos and compared them to Facebook's "database of user face templates," if a match was found, Facebook would "suggest tagging the person in the photo."[13]

The 9th Circuit held that standing ought to be conferred because the plaintiffs "alleged a concrete injury-in-fact sufficient to confer Article III standing."[14] First the 9th Circuit determined that Facebooks alleged violations "invades an individual's private affairs and concrete interests."[15] The court emphasized the various ways facial mapping technology could be used to invade one's privacy from unlocking their phone to tracking them via real-time surveillance.[16] Next, the 9th Circuit concluded that a mere procedural violation of BIPA could constitute an injury-in-fact because "the procedural protections in BIPA 'are particularly

crucial in our digital world' because '[w]hen a private entity fails to adhere to the statutory procedures … the right of the individual to maintain his or her biometric privacy vanishes into thin air.'"[17]

It is clear from the 9th Circuit and Illinois Supreme Court rulings that the enforcement provision of BIPA is extremely strong. Even claims which only allege technical or procedural BIPA violations are actionable.

Interestingly, a federal district court in Illinois (in the 7th Circuit) seemingly veered from the 9th Circuit's decision in *Facebook*. *Bryant v. Compass* presented the same issue regarding the extent of injury required to satisfy Article III standing in a BIPA case. Plaintiffs alleged that Compass vending machines required users to provide fingerprints in order to purchase items.[18] Citing Northern District of Illinois precedent, the court concluded that the plaintiffs lacked Article III standing because the fingerprints were only used as the plaintiff expected and were not used for any other purpose nor distributed to a third party.[19]

The court distinguished *Facebook* because the plaintiffs there had no reason to anticipate that photos they posted would be analyzed and stripped for their facial template, whereas in the present case, the fingerprint was only used in the way known and anticipated by the plaintiffs.[20] The Court concluded by holding that establishing that one is an "aggrieved person" who is entitled to relief under BIPA does not necessarily establish that the individual would have Article III standing in federal court. Since there were no "actual injuries" and the only BIPA violations were simply procedural in nature (lack of written consent and lack of a written policy), there could not be Article III standing.[21]

BIPA "has proven to be remarkably long-sighted and resistant to attempts by industry (including, apparently, by Facebook while it fought its own court battle) to water it down."[22] Although the legislature and courts have stressed the strong policy reasons behind BIPA, is the ease of bringing a BIPA claim problematic? The magnitude of potential damages which could result from the misuse of biometric data surely create a strong need for legislation that promotes deterrence to the highest degree as BIPA does.

The importance of encouraging private entities to comply with all aspects of BIPA cannot be overstated. Even if a private entity collecting biometric data is without malicious intent, it is extremely important to protect the data from bad actors who may wish to hack these private entities. Complying with BIPA would likely reduce the risk of biometric data being compromised by requiring policies which detail the eventual permanent deletion of said data and notification requirements which afford individuals the chance to opt out of providing their biometric data if they so choose.

Though enforcement against BIPA violators is of high importance, individuals who are unable to allege any actual damages outside a mere technical violation of their rights under BIPA

should not be afforded a cause of action by the legislature. Instead of allowing a private cause of action where no actual damages were endured, Illinois should only provide a right of action to the attorney general. Without such a limitation, unharmed plaintiffs are motivated to bring BIPA suits against potentially innocent companies who will either be forced into expensive and lengthy litigation in an attempt to clear their name or settle for high amounts – neither outcome should be acceptable.

Experts have predicted that the floodgates will continue to open and BIPA suits will continue to arise in 2020, and so far, their predictions have come true.[23]

This past January, on the heels of the 9th Circuit's determination that the plaintiffs in *Patel v. Facebook* had Article III standing, Facebook announced that they would settle the suit for $550 million.[24] Soon after the settlement was announced a number of high-profile BIPA cases were filed.

On February 6, 2020, a class action suit was filed against Google in the Northern District of California.[25] Similar to *Facebook*, the suit alleges that Google creates facial templates from photos uploaded to Google Photos and applies facial recognition technology to those photos and templates without obtaining written consent from users.[26]

On February 13, 2020, a class action suit was filed against Clearview AI in New York.[27] The suit alleges that Clearview AI "actively collected, stored and used Plaintiffs' biometrics — and the biometrics of most of the residents of Illinois — without providing notice, obtaining informed written consent or publishing data retention policies."[28] Clearview AI is a start-up that has scraped the internet for public images for the purpose of subjecting it to facial recognition technology. They have developed an app that allows a user to take a picture of a person, upload it to the app, and the app will show the user all public photos of that person along with links to said pictures.[29] Law enforcement has used Clearview AI to solve a number of criminal cases.[30]

With the high BIPA damages, the ease of a company violating BIPA and the low bar required to bring a BIPA suit, the influx of BIPA cases will likely continue, putting all companies who use any type of biometric data subject to BIPA at a very high risk of costly litigation or settlement.

It will be interesting to see how other states tackle the issue of biometric data privacy and whether other state follow the lead and draft tough-on-violators, BIPA-like, legislation. Further, monitoring how other district courts tackle the Article III standing issue is important as well, tracking whether the courts follow the lead of the *Compass* court and trend towards raising the bar for plaintiffs, or whether they will continue to trend towards a lower bar like *Rosenbach* and *Facebook*.

Zack Perlitsh is a Second Year Law Student at the Benjamin N. Cardozo School of Law and a Staff Editor at the Cardozo Arts & Entertainment Law Journal. Zack is interested in corporate law, asset management, and privacy & data law.

---

[1] 740 Ill. Comp. Stat. Ann. 14/15 (West).

[2] *Id.*

[3] *Id.*

[4] 740 Ill. Comp. Stat. Ann. 14/20 (West).

[5] *Id.*

[6] 740 Ill. Comp. Stat. Ann. 14/5 (West).

[7] *Id.*

[8] *Id.*

[9] Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197 (Ill. 2019).

[10] *Id.* at 1201.

[11] *Id.* at 1207.

[12] Patel v. Facebook, Inc., 932 F.3d 1264, 1268 (9th Cir. 2019), cert. denied, No. 19-706, 2020 WL 283288 (U.S. Jan. 21, 2020).

[13] *Id.*

[14] *Id.* at 1274.

[15] *Id.* at 1273.

[16] *Id.*

[17] *Id.* at 1274 (quoting Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197, 1206 (Ill. 2019)).

[18] Bryant v. Compass Grp. USA, Inc., No. 19 C 6622, 2020 WL 433868, at *1 (N.D. Ill. Jan. 28, 2020).

[19] *Id.* at *4.

[20] *Id.* at *8

[21] *Id.* at *10

[22] Devin Coldewey, *Class Action Suit Against Clearview AI Cites Illinois Law that Cost Facebook $550M*, TechCrunch (Feb. 14, 2020), https://techcrunch.com/2020/02/14/class-action-suit-against-clearview-ai-cites-illinois-law-that-cost-facebook-550m/.

[23] Jeffrey Rosenthal & David Oberly, Biometric Privacy In 2020: The Current Legal Landscape, Law360 (Feb. 3, 2020, 5:59 PM), https://www.law360.com/articles/1239794?scroll=1&related=1.

[24] Jim Nash, *Facebook Settles Biometric Face-Tagging Suit for $550 Million*, BiometricUpdate.com (Jan. 29, 2020), https://www.biometricupdate.com/202001/facebook-settles-biometric-face-tagging-suit-for-550-million.

[25] Ross Todd, *Google Hit With Class Action Under Illinois Biometric Privacy Law Over Facial Recognition*, Law.com (Feb. 7, 2020 at 12:32PM), https://www.law.com/therecorder/2020/02/07/google-hit-with-class-action-under-illinois-biometric-privacy-law-over-facial-recognition/?slreturn=20200123042141.

[26] *Id.*

[27] Coldewey *supra* note 22.

[28] *Id.*

[29] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, NY Times (Updated Feb. 10, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[30] *Id.*