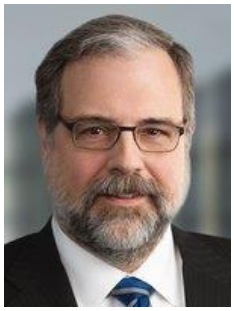
Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

BIPA May Apply To Clearview AI's Creation Of Biometric Data

By **Al Fowerbaugh and Karen Borg** (February 18, 2020, 5:28 PM EST)



Al Fowerbaugh

Karen Borg

Eleven years ago, Illinois enacted the Biometric Information Privacy Act.[1] BIPA requires a person or business to make certain disclosures to, and receive a written release from, a person before obtaining his or her biometric identifier — a fingerprint, voiceprint, a scan of a person's retina, iris, or hand, or the person's facial geometry — or biometric information — information derived from a biometric identifier used to identify that person.[2]

BIPA also requires those possessing biometric identifiers or information to develop a publicly available, written retention policy establishing a schedule and guidelines for the destruction of the biometric identifiers and information and prohibits them from selling or leasing that information.[3] Anyone violating a provision of BIPA is liable for the greater of either actual damages incurred, or statutory penalties of $1,000 per negligent violation, or $5,000 per willful violation, plus attorney fees.[4]

BIPA spent most of that time in obscurity. As biometric technology advanced and its use became more common, few people were aware of, or complied with, BIPA's requirements. That, however, changed in January 2019, when the Illinois Supreme Court held in Rosenbach v. Six Flags Entertainment Corp. that "an individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to … seek liquidated damages and injunctive relief" under BIPA.[5]

With plaintiffs now able to bring lawsuits seeking statutory penalties up to $5,000 for each alleged violation of BIPA, without having to allege they suffered an actual injury resulting from those violations, the number of class actions brought under BIPA exploded.

These cases were brought primarily against those who directly collected the biometric identifiers or biometric information from the plaintiffs, such as employers that required employees to use their fingerprints to clock in and clock out of work. The plaintiffs also sued Shutterfly Inc., Google Inc. and Facebook Inc., which allegedly derived biometric facial geometries from the photographs the plaintiffs uploaded to their websites.

However, only recently have plaintiffs attempted to assert claims under BIPA against parties who did not have any direct dealings with the plaintiffs. Rather, these defendants are alleged to have created

biometric information from photographs and other data they independently obtained from social media websites.

The lawsuits against these defendants present a number of issues not raised in the typical lawsuits brought against those that directly obtain biometric identifiers or biometric information from the plaintiffs. This article will identify and discuss some of those issues.

The Lawsuits Against Clearview AI and IBM

On Jan. 18, the New York Times published a story about Clearview AI, a company that amassed a database of over 3 billion photographs of people that were posted to Facebook, YouTube Inc., Venmo LLC and other websites.[6] Clearview AI reportedly used a "state-of-the-art neural net" to convert these images into mathematical formulas based upon the images' facial geometries.[7]

Customers, such as law enforcement, could upload a person's image and Clearview AI's system could identify that person as well as provide its customer with all the images of that person that Clearview obtained from the various websites, along with links to the websites where those images originated.[8]

Four days after the New York Times article was published, a class action was filed against Clearview AI in the U.S. District Court for the Northern District of Illinois, asserting four counts of violation of BIPA, along with claims for various constitutional violations.[9] The plaintiff, David Mutnick, alleges that he and the other class members are Illinois residents whose images appear "in numerous internet-based platforms and websites" and that Clearview AI took those images from those websites and created facial geometries of his and the other class members from those images without obtaining his and class members' prior written consent.[10]

The plaintiff also asserts that Clearview AI violated BIPA by not providing him and the class members with the required disclosures, by not having the required retention policy and by profiting from the sale or leasing of the biometric information or identifiers.[11] As such, the plaintiff seeks classwide damages of the greater of either statutory or actual damages, along with injunctive relief and attorney fees.

Two weeks after the Mutnick complaint was filed, a second plaintiff, Anthony Hall, commenced another action against Clearview AI, making similar allegations and asserting similar claims against Clearview AI under BIPA.[12]

On the same day the Mutnick complaint was filed, a similar case was commenced against International Business Machines Corp. in the Circuit Court of Cook County, Illinois.[13] The plaintiff, Tim Janecyk, likewise alleges that IBM obtained approximately 1 million pictures from Yahoo, which in turn obtained those photographs from the Flickr website and created and stored facial geometries of those images in a database.[14]

Janecyk claims that IBM violated BIPA by not providing him or the class the required disclosures, by not obtaining his or the class members' prior written consent, by not publicly providing a retention schedule governing this information and by making this information publicly available.[15]

Based on these allegations, Janecyk seeks classwide damages of the greater of either statutory or actual damages, along with injunctive relief and attorney fees. Two days later, a second plaintiff, Steven Vance, commenced an action against IBM in the Northern District of Illinois, making similar allegations and asserting similar claims against IBM under BIPA.[16]

Do the defendants possess biometric information or biometric identifiers?

A basic requirement for a claim under BIPA is that the defendant possess either biometric identifiers or biometric information.[17] The allegations in the Mutnick, Hall, Janecyk and Vance complaints, that Clearview AI or IBM possess the plaintiffs' and the class members' facial geometries, would seem to be sufficient to satisfy this requirement because "face geometry" is included in the definition of biometric identifier.[18]

However, none of the plaintiffs allege that the defendants obtained facial geometries directly from them or from a third party. Rather, the plaintiffs allege that Clearview AI and IBM obtained photographs of them and the class members from third-party websites.[19] Since photographs are expressly excluded from BIPA's definition of a biometric identifier,[20] a court could conclude that the defendants did not possess biometric identifiers of the plaintiffs.

That, however, is not the end of the analysis. The plaintiffs also allege that, through the use of various computer algorithms, the defendants derived facial geometries from the photographs, and the resultant facial geometries constitute either biometric identifiers or biometric information.[21]

"Biometric information" is defined as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual."[22] However, biometric information "does not include information derived from items or procedures excluded under the definition of biometric identifiers."[23]

Since the plaintiffs allege that the facial geometries were derived from photographs, which are excluded from the definition of biometric identifiers, a court could conclude that the facial geometries derived from these photographs are not "biometric information" as defined under BIPA.

Thus, the conundrum courts may have to resolve is whether the facial geometries allegedly in the defendants' possession are covered by BIPA. On the one hand, facial geometries are expressly covered under BIPA, and the plaintiffs' allege that Clearview AI and IBM possess facial geometries. On the other hand, none of the plaintiffs allege that the defendants collected their facial geometries.

Rather, all that was allegedly obtained were photographs, which are excluded from the definition of biometric identifiers, and the information derived from the photographs are expressly excluded from the definition of biometric information. The court in the In re Facebook Biometric Info. Privacy Litigation held that similar allegations were sufficient to state a claim for violation of BIPA under federal pleading standards.[24]

However, the court also noted its ruling was based solely upon the plaintiffs' allegations and stated that later discovery may show "that 'scan' and 'photograph' with respect to Facebook's practices take on technological dimensions that might affect BIPA claims."[25]

Thus, the court appeared to be open to the possibility that evidence may later demonstrate that data derived from photographs may not constitute a biometric identifier. However, at least two other courts later held that, by its terms, BIPA encompasses facial geometries derived from photographs.[26]

Does BIPA apply to conduct occurring outside Illinois?

In addition to determining whether the defendants obtained biometric identifiers or information, a court will likely have to determine if BIPA applies to alleged conduct occurring outside of the state of Illinois.

It has long been the rule in Illinois that a "statute is without extraterritorial effect unless a clear intent in this respect appears from the express provisions of the statute."[27] If the statute is not given extraterritorial effect, it is "operative only as to persons or things within Illinois."[28] An alleged violation of BIPA will be determined to have occurred in Illinois "if the circumstances relating to the transaction occur primarily and substantially" within Illinois.[29]

There is nothing in BIPA that expressly states that it was intended to apply to actions taken outside of Illinois. To the contrary, the legislative findings included in BIPA suggest the General Assembly was concerned with the use of biometric information within Illinois:

Major national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias.[30]

The plaintiffs in the Mutnick, Hall, Janecyk and Vance cases make few allegations showing that the defendants' alleged BIPA violations occurred in Illinois. Although they and the purported class members are Illinois residents, none of the defendants are alleged to be Illinois citizens,[31] although IBM is alleged to have had a "large and continuous presence in Illinois for many years."[32]

While the plaintiffs allege that they uploaded the photographs to third-party websites, none of them allege the location where those websites stored the photographs that were allegedly taken by the defendants. The plaintiffs also do not allege where the defendants conducted the analysis of the photographs that created the facial geometries at issue, nor do they allege where the defendants stored those photographs or biometric data.

Likewise, there are few allegations showing that the defendants used or disclosed the biometric data in Illinois. While the plaintiffs in the Janecyk and Vance actions allege that IBM made its facial geometry database available to third-party researchers, they do not allege that this database was provided to researchers in Illinois.[33] The plaintiff in the Mutnick action alleges that Clearview entered into service agreements with over 600 law enforcement agencies.[34]

Although the plaintiff does not allege the locations of all these agencies, he does allege that one of them is the Springfield, Illinois police department.[35] The plaintiff in the Hall action also alleges that Clearview AI made its database available to the Chicago police department.[36]

The courts may be required to determine whether the plaintiffs' allegations, especially in the Janecyk and Vance complaints, or the facts as developed through discovery, are sufficient to establish the necessary connection between the defendants or their alleged conduct and Illinois. The courts that addressed this issue have agreed that BIPA does not have extraterritorial application.

For example, in the In re Facebook Biometric Information Privacy Litigation, the court noted that "the parties agree that BIPA does not have extraterritorial reach because no 'clear intent in this respect appears from the express provisions of the statute.'"[37] However, the court further noted that the

parties disagreed as to the application of that rule to the facts of the case.[38]

Other courts have likewise agreed that BIPA is not to be given extraterritorial application, but found that the question of whether the alleged violations occurred "primarily and substantially within Illinois" involved factual questions unique to each case.[39]

Are Clearview AI's dealings with police departments in Illinois exempted from BIPA?

As mentioned above, the plaintiffs in the Mutnick and Hall actions allege that Clearview AI entered into a service agreements or otherwise made its database available to the Springfield, Illinois and Chicago police departments.[40]

While these allegations establish conduct within Illinois, the court will likely have to decide whether this alleged conduct is actionable in light of the provision in BIPA that "[n]othing in this Act shall be construed to apply to a contractor, subcontractor, or agent of a State agency or local unit of government when working for that State agency or local unit of government."[41]

Although BIPA does not define the phrase "local unit of government," the Illinois constitution defines it as "counties, municipalities, townships, special districts, and units, designated as units of local government by law, which exercise limited governmental powers or powers in respect to limited governmental subjects, but does not include school districts."[42]

Although Chicago and Springfield clearly fit within this definition, a court will have to decide whether the police departments of those cities likewise fall within the scope of this exemption. This will turn on which definition of "local unit of government" a court relies upon.

For example, in a dissent one appellate justice, relying on the definition in the Illinois constitution, stated that the "Chicago police department and the police board are not units of local government under Illinois law."[43] However, not all courts have applied the constitutional definition of "local unit of government" to all statutes.

For example, police officers have been held to be employees of "a unit of local government" in connection with the criminal statute defining aggravated battery as the battery of an "officer or employee of the State of Illinois, a unit of local government, or a school district."[44] A court could also bypass this issue and find that a police department is a division of a city government and thus falls within the scope of this exemption.[45]

Finally, if a court determines this exemption applies, it must also determine the scope of that exemption. If the court narrowly construes and applies that exemption, then the exemption may apply only to the claim that Clearview AI violated BIPA by profiting from the biometric data through its agreement with a police department. If so, then claims relating to the alleged failure to provide the required disclosures, obtain the required written consent and establish publicly available retention policies may proceed.

If, however, the court broadly construes this exemption, then the court may conclude that it bars any claims under BIPA in any way connected to the transaction with the police department.

Conclusion

The Illinois General Assembly enacted BIPA because the "overwhelming majority of members of the public are weary of the use of biometrics," the "full ramifications of biometric technology are not fully known," and "public welfare, security, and safety will be served" by regulating the use of biometric information.[46] Those concerns are just as valid today.

However, people now share far more information about, and images of, themselves on social media that can be harvested by third parties and used to create a database that can identify millions of people worldwide. The internet enables this to occur anywhere, yet BIPA is limited to the use of biometric information occurring in Illinois.

These emerging technologies may allow police departments or governmental agencies to engage in widespread surveillance of the population, yet it is unclear whether BIPA applies to this use of our biometric data. The resolution of the issues arising from cases such as the Mutnick, Janecyk and Vance cases will show to what extent BIPA applies to these new technologies and uses of biometric data.

Al Fowerbaugh and Karen Borg are partners at Porter Wright Morris & Arthur LLP.

[1] 740 ILCS 14/1, et seq.

[2] 740 ILCS 14/10, 14/15.

[3] 740 ILCS 14/15.

[4] 740 ILCS 14/20.

[5] 2019 IL 123186, ¶ 40 (2019).

[6] Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," New York Times (January 18, 2020), available at https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[7] Id.

[8] Id.

[9] Mutnick v. Clearview AI, Inc., et al., No. 1:20-cv-00512 (N.D. Ill. January 22, 2020).

[10] Mutnick Complaint, ¶¶ 2, 12.

[11] Id. at ¶¶ 99, 106, 113.

[12] Hall v. Clearview AI, et al., No. 1:20-cv-00846 (N.D. Ill. February 5, 2020).

[13] Janecyk v. International Business Machines Corporation, No. 2020 CH 00833 (Circuit Court of Cook County, Chancery Division) (January 22, 2020).

[14] Janecyk Complaint, ¶¶ 5, 6.

[15] Id. at ¶¶ 53-56

[16] Vance v. International Business Machines Corporation, No. 1:20-cv-00577 (United States District Court for the Northern District of Illinois) (January 24, 2020).

[17] See 740 ILCS 15(a) ("A private entity in possession of biometric identifiers or biometric information …"); 740 ILCS 15(b) ("No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or customer's biometric identifier or biometric information, unless …"); 740 ILCS 15(c) ("No private entity in possession of a biometric identifier or biometric information …"); 740 ILCS 15(d) ("No private entity in possession of a biometric identifier or biometric information …").

[18] 740 ILCS 10.

[19] Mutnick Complaint, ¶¶ 7, 33; Janecyk Complaint, ¶¶ 5, 23; Vance Complaint, ¶¶ 4, 30; Hall Complaint, ¶¶ 2, 11.

[20] 740 ILCS 10 ("Biometric identifiers do not include … photographs …").

[21] Mutnick Complaint, ¶¶ 2, 34; Janecyk Complaint, ¶¶ 6, 25; Vance Complaint, ¶¶ 4, 33; Hall Complaint ¶¶ 3, 13.

[22] 740 ILCS 14/10.

[23] Id.

[24] In re Facebook Biometric Info. Privacy Litigation, 185 F. Supp. 3d 155, 1172 (N.D. Cal. 2016).

[25] Id.

[26] Rivera v. Google Inc., 238 F. Supp. 3d 1088, 1096-1097 (N.D. Ill. 2017); Monroy v. Shutterfly, Inc., 2017 U.S. Dist. LEXIS 149604, at *5-*14 (N.D. Ill. Sept. 15, 2017).

[27] Avery v. State Farm Mut. Auto. Ins. Co., 216 Ill. 2d 100, 184-85 (2005).

[28] Stroman Realty, Inc. v. Allison, 2017 IL App (4th) 150501-U, ¶ 59.

[29] Avery, 216 Ill. 2d at 186.

[30] 740 ILCS 14/5(b).

[31] Clearview is alleged to be a Delaware corporation with its headquarters in New York. Mutnick Complaint, ¶ 13; Hall Complaint ¶ 9. IBM is alleged to be a citizen of the State of New York. Vance Complaint, ¶ 12; Janecyk Complaint, ¶ 9.

[32] Vance Complaint, ¶ 14.

[33] Vance Complaint, ¶¶ 35-38; Janecyk Complaint, ¶ 27.

[34] Mutnick Complaint, ¶ 37.

[35] Id.

[36] Hall Complaint, ¶ 6.

[37] In re Facebook Biometric Info. Privacy Litigation, 326 F.R.D. 535, 547 (N.D. Cal. 2018), quoting Avery v. State Farm Mut. Auto. Ins. Co., 216 Ill. 2d 100, 185 (2005).

[38] Id.

[39] Monroy v. Shutterfly, Inc., 2017 U.S. Dist. LEXIS 149604) (N.D. Ill. Sept. 15, 2017); Neals v. Par Tech. Corp., 2019 U.S. Dist. LEXIS 220907 (N.D. Ill. Dec. 18, 2019); Rivera v. Google, Inc., 238 F. Supp. 1088 (N.D. Ill. 2017).

[40] Mutnick Complaint, ¶ 37; Hall Complaint, ¶ 6. The plaintiff in the Hall action also alleges that Clearview AI entered into a contract with co-defendant CDW Government LLC, an Illinois corporation, to lease Clearview AI's database to third-parties. Hall Complaint, ¶¶ 10, 41. Although Hall alleges that Clearview AI "sells or leases access to the surveillance database to public and private entities for profit," Id. at ¶ 16, he does not allege the identity of any customer other than the Chicago police department.

[41] 740 ILCS 14/25(e).

[42] Ill. Const. 1970, art. VII, § 1.

[43] Lesner v. Police Bd., 2016 IL App (1st) 150525, ¶ 58 (dissent).

[44] 720 ILCS 5/12-3.05(d)(6); People v. Sanchez, 2014 IL App (1st) 120514.

[45] Jordan v. Chicago, Dep't of Police, 505 F. Supp. 1, 4 (N.D. Ill. 1980) ("Chicago Police Department is not a suable entity, but merely a department of the City of Chicago which does not have a separate legal existence.")

[46] 740 ILCS 14/5 (d), (f), (g).