Articles + Publications | July 6, 2022

BIPA's Scope Shaped by Courts With No Legislative Relief in Sight

Privacy & Cybersecurity Newsletter

WRITTEN BY

Kenneth K. Suh | Hannah Oswald

Since the Illinois Supreme Court's *Rosenbach* decision[1] holding that BIPA[2] is actionable on the mere showing of statutory violations rather than actual harm, litigants and courts alike have been busy shaping BIPA case law. Here are issues about which courts have ruled.

Broad Definitions of "Biometric Identifier" and "Biometric Information"

BIPA regulates the collection, sale, disclosure, consent, and destruction of biometric data under two categories, "biometric identifier[s]" and "biometric information." "Biometric identifier" includes certain immutable physical characteristics of a person—"retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[3] "Biometric information" is defined broadly as "any information…used to identify an individual" that is "based on an individual's biometric identifier[,]"[4] which at least implies that BIPA regulates any non-anonymized result of a computational analysis of a person's biometric identifiers.

While BIPA expressly excludes certain types of data, including "photographs," courts have narrowly interpreted these exclusions, for example by holding that "unique numerical representations" based on a person's facial geometry that was derived from a photograph constitutes a "biometric identifier."[5]

Specific Disclosure and Consent

Recent case law has clarified BIPA's disclosure and consent requirements.[6] Businesses must disclose and receive consent for the specific biometric identifier or biometric information they collect or derive from data that is collected. For example, blanket consent to collect photographs will likely be insufficient to fulfill the requirement to seek consent on the types of biometric identifiers or information might be derived from the photographs.[7]

Limitation of BIPA

Thus far, courts have found a handful of fact-specific limitations to BIPA's statutory scheme:

<u>Pre-emption</u>: Union employees' allegations of BIPA violations by their employer are pre-empted by the (Federal) Labor Management Relations Act so long as the employee and employer had a collective bargaining agreement in place.[8] However, BIPA is not pre-empted by the Illinois Workers' Compensation Act.[9]

Similarly, a Federal Court has ruled that the Airline Deregulation Act pre-empts BIPA allegations raised by a passenger against an airliner for collecting biometric data in connection with voice response software.[10]

Contact: The complainant and business must have some relationship. “[A]t least some measure of knowing contact with and awareness of the people subject to biometric data collection” must exist with the business that is collecting biometric data in order for the business to be subject to BIPA.[11] That is, BIPA does not require entities to proactively identify persons whose biometric data may be in their possession, for example because a user of a social media website uploaded pictures including non-users.[12]

Arbitration Clauses: While not a legal defense, businesses can avoid costly and broad class action litigation. Businesses may prefer resolving alleged BIPA violations through arbitration with individual complainants in less public forums.[13] In *Whalen*, the court granted Facebook’s motion to compel arbitration because the plaintiff assented to Instagram’s terms of use, including terms that were disclosed to the plaintiff through an in-app update.[14]

Undecided Issues

Number and accrual of violations:

The Illinois Supreme Court is expected to decide in the fall of 2022 whether a violation of BIPA occurs each time a person’s biometric identifier is scanned or only the first time a person’s biometric identifier is scanned by a particular entity.[15] A “per scan” ruling by the Court coupled with the statutory damages could exponentially increase the liability exposure for BIPA violations.

Statute of limitation: The Illinois Supreme Court also has pending a case that would decide the applicable statute of limitations for BIPA—either the state’s general five year statute of limitations, which applies to civil cases unless otherwise prescribed by law, the state’s one year statute of limitations, which applies alleged privacy violations involving publication, or some combination.[16] In 2021, an appellate court ruled that BIPA’s provisions involving alleged improper publication of biometric data are subject to a one year statute of limitations, while the remaining provisions are subject to a five year statute of limitations.

Other pre-emption: A case involving Google before Central District of Illinois will likely decide whether BIPA is pre-empted by the Federal Children’s Online Privacy Protection Act (“COPPA”) and Illinois Student Online Personal Protection Act (“SOPPA”), which regulate the online collection of personal information from children under the age of 13.[17] The case involves Google education products which were distributed by schools to minor children.

“Profit” under BIPA: A case involving Macy’s and their use of a facial recognition vendor for loss prevention will likely decide the breadth of BIPA’s seemingly blanket prohibition against “sell[ing], leas[ing], trad[ing], or otherwise profit[ing] from a person’s or a customer’s biometric identifier or biometric information.”[18] Importantly, companies cannot avoid this prohibition with informed consent.

Conclusion

While legislative attempts to clarify or rein in BIPA’s reach have failed to date, litigation continues to shape

BIPA's impact on entities conducting business in Illinois or with Illinois residents. Among other examples, proposed legislation to limit damages[19] and clarify the timing of BIPA's informed consent requirement for repeated collections of biometric data[20] have both not progressed very far.

Entities should carefully assess whether BIPA applies to their activities, including with their customers and employees, and take measures to ensure compliance. As courts have tended to apply BIPA's requirements broadly and narrowly apply any exclusions, compliance with the statute's notice and consent requirements remains the best legal risk management course.

***

?[1] *Rosenbach v. Six Flags Entertainment Corp*., 2019 IL 123186 (2019).

?[2] See Locke Lord companion articles about laws in other states that address the privacy of biometric information and the growing case law concerning disputes over insurance coverage for BIPA claims.

?[3] 740 ILCS 14 Sect. 10.

?[4] 740 ILCS 14 Sect. 10.

?[5] *Sosa v. Onfido, Inc*., Case No. 20-cv-4247 (N.D. Ill Apr. 25, 2022).

?[6] 740 Ill. Comp. Stat. 15(a) (disclosure requirement) and 14/15(b) (consent requirement).

?[7] *Sosa v. Onfido, Inc*., Case No. 20-cv-4247, (N.D. Ill. Apr. 25, 2022).

?[8] *Walton v. Roosevelt University,* 2022 IL App (1st) 210011 (1st Dist. 2022).

?[9] *McDonald v. Symphony Bronzeville Park, LLC, et al*., 2022 IL 126511 (2022).

?[10] *Alex Kislov et al. v. American Airlines Inc.*, Case No. 1:17-cv-09080, Dkt. 111 (N.D. Ill. Mar. 22, 2022).

?[11] *Zellmer v. Facebook Inc*., Case No. 3:18-cv-01880 (N.D. Cal. April 1 2022).

?[12] *Zellmer v. Facebook Inc*., Case No. 3:18-cv-01880 (N.D. Cal. April 1 2022).

?[13] *Kelly Whalen et al. v. Facebook Inc*., Case No. 4:20-cv-0636 (N.D. Cal. Apr. 4, 2022).

?[14] *Kelly Whalen et al. v. Facebook Inc*., Case No. 4:20-cv-0636 (N.D. Cal. Apr. 11, 2022). *See also K.F.C. v. Snap Inc*., Case No. 21-2247 (7th Cir. 2022).

?[15] *Cothron v. White Castle Sys., Inc*., 20 F.4th 1156 (7th Cir. 2021), *argued Cothron v. White Castle System Inc*., Case No. 128004.

?[16] 735 ILCS 5/13-205, 735 ILCS 5/13-201, *Tims v. Black Horse Carriers, Inc*., 2021 IL App (1st) 200563, *appeal filed* Case No. 127801.

?[17] *H.K. et al. v. Google LLC*, case number 1:21-cv-01122 (C.D. Ill. Apr. 1, 2022).

?[18] *In Re: Clearview AI Inc. Consumer Privacy Litigation*, Case No. 1:21-cv-00135. Dkt. 314 (N.D. Ill. Mar. 18, 2022).

?[19] 2021 HB 0559

?[20] 2022 SB 3874

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber