



May 03, 2023

Categories:

[Class Action Defense](#)
[Privacy Class Actions](#)

Delaware District Court Allows for Single Claim to Proceed Against Amazon in Illinois Biometric Information Privacy Act Class Action Suit

The Illinois [Biometric Information Privacy Act](#) (BIPA) is designed to protect and regulate the use of both “biometric identifiers” and “biometric information” of Illinois residents. “Biometric identifiers,” for instance, include “a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.” In contrast, “biometric information” means “any information ... based on an individual’s biometric identifier used to identify an individual.” On March 29, 2023, in [McGoveran v. Amazon Web Servs., Inc.](#), the United States District Court for the District of Delaware granted in part Amazon Web Services (“Amazon”) and Pindrop Security’s (“Pindrop”) motion to dismiss a proposed class action brought pursuant to BIPA for lack of standing, based on a strict interpretation of the definitions of “biometric identifiers” and “biometric information” and the plaintiffs’ failure to adequately allege that they suffered any concrete, actual, or imminent injury as a result of the defendants’ conduct.

In *McGoveran*, a group of Illinois residents alleged that Amazon and Pindrop violated BIPA by extracting their biometric information for authentication purposes when the plaintiffs called John Hancock to discuss their retirement accounts. At the outset, the court held that the plaintiffs lacked Article III standing to bring a claim under BIPA Section 15(a) and Section 15(c) or to otherwise obtain injunctive relief. Under Section 15(a), a company is required to both develop a written data-retention policy for the processing of biometric information *and* destroy biometric information that is no longer being used or within three years of the individual’s last interaction with the company. Under Section 15(c), a company is also prohibited from profiting from someone’s biometric information. Though the plaintiffs alleged that the defendants failed to develop a

written data-retention policy, the court found that “[t]he statutory duty to develop and make available a written policy ‘is owed to the public generally, not to particular persons whose biometric information the entity collects,’” and thus “failing to follow section 15(a)’s written-policy requirement does not injure individual plaintiffs in ‘a concrete and particularized’ way.” Further, the complaint’s allegations were “not enough for standing” because the complaint failed to allege that: (1) the defendants no longer needed their biometric information; (2) the defendants’ actions prevented them from otherwise profiting from their own biometric information; or (3) the defendants’ actions caused the plaintiffs continuing or imminent harm.

Albeit on other grounds, the court likewise dismissed the plaintiffs’ claim brought under Section 15(d), which prohibits companies from disseminating an individual’s biometric identifier or biometric information. The plaintiffs alleged that Amazon violated this provision “by sharing their voice audio with Pindrop.” As the court explained, however, “voice audio alone is neither a biometric identifier (a voiceprint) nor biometric information (information derived from a voiceprint)” under BIPA. As the plaintiffs failed to allege that Amazon shared its “voiceprints, or that it shared any information based on voiceprints that could be used to identify them,” they failed to state a claim.

In contrast, however, the court held the plaintiffs’ Section 15(b) claim against Amazon could proceed. Under Section 15(b), covered entities are prohibited from “‘collect[ing]’ biometric data without first getting written informed consent.” Accordingly, as the plaintiffs alleged “that Amazon itself extracts voiceprints and uses them to authenticate callers, all without informed consent,” the court denied Amazon’s motion to dismiss on this count of the plaintiffs’ complaint.

The *McGoveran* decision illustrates how Article III standing should remain the operative focus of any privacy class action defense. While BIPA provides a private right of action for liquidated damages and attorneys’ fees and costs, as *McGoveran* instructs, plaintiffs are still required to allege that their injury is “actual or imminent” or,

indeed, “*certainly impending*.” Therefore, companies should seek to maintain strong compliance processes, especially when informed consent is required at the time of collection.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.