

“Possess” or “Collect” under Illinois’ BIPA: Seventh Circuit Resolves Trial–Court Split

by Sophia Mancall-Bitel, Matthew D. Provance,
Tony Weibell, and Riley P. Harkin

In a decision that cuts against the trend of expansive readings of the Biometric Information Privacy Act (“BIPA”), the U.S. Court of Appeals for the Seventh Circuit has held that a company does not “possess” or “collect” biometric data merely by supplying software that creates or processes such data on a user’s own device. In *G.T. v. Samsung Electronics America, Inc.*, the district court dismissed the complaint with prejudice for failure to state a claim, finding that plaintiffs had not plausibly alleged that Samsung possessed or collected face templates that the preinstalled Gallery app generated and stored on users’ phones. The Seventh Circuit affirmed, holding that possessing, collecting, capturing, and obtaining biometric data under BIPA all require the defendant to have some degree of control over that data. The decision represents a significant development for device manufacturers, app developers, and other companies whose products may generate biometric data on user hardware.

Background

BIPA Section 15(a) applies to a private entity “in possession of” biometric identifiers or biometric information, and Section 15(b) applies to one that “collect[s], capture[s], purchase[s], receive[s] through trade, or otherwise obtain[s]” it. Defendants have argued that these terms exclude technologies that create and process biometric data solely on a user’s own device, as opposed to those that process the data on the company’s own servers. Until now, however, the law on the question remained unsettled in the Seventh Circuit, where a majority of BIPA litigation is filed or removed pursuant to the Class Action Fairness Act (“CAFA”).

Two lines of cases had emerged. Representing one side, in *Hazlitt v. Apple Inc.*, 543 F. Supp. 3d 643 (S.D. Ill. 2021), the court held that plaintiffs adequately alleged possession under Section 15(a) where they alleged that Apple’s Photos app stored faceprints in on-device databases that users could not access; that users could neither delete the data nor disable the feature; that users had to accept the collection in order to use the devices at all; and that Apple alone could access the data or disable its collection. That was enough, the court held, to allege “complete and exclusive control over the data on Apple Devices.”

On the other side, in *Bhavilal v. Microsoft Corp.*, 716 F. Supp. 3d 640 (N.D. Ill. 2024), the court dismissed Sections 15(a) and 15(b) claims against Microsoft over facial-scanning software in Windows, holding that “control of the facial scan software is not the same as control of the facial scan data that is collected using the software,” and that “selling or licensing a tool that can be used to collect a facial scan

is not the same as actually doing the collecting.” The plaintiff’s theory, the court concluded, “conflates two different activities—providing the tool versus using the tool.”

An Illinois appellate court took a similar view in *Barnett v. Apple Inc.*, 2022 IL App (1st) 220187, affirming dismissal of Sections 15(a) and 15(b) claims over the fingerprint and facial recognition features on Apple devices. The court reasoned that Apple did not “possess” biometric data just because Apple’s software processed it, holding that the user—not the company—is the one who captures her own biometric information using the device as a tool. Ultimately, the tension between these approaches set the stage for *G.T. v. Samsung*.

The Seventh Circuit Decision

The plaintiffs bought and used Samsung smartphones and tablets and brought a putative class action on behalf of Illinois residents. They alleged that the preinstalled Gallery app automatically scans saved photographs for faces and creates a “face template” capturing each face’s unique geometry, then matches templates across photos to cluster images of the same person. The plaintiffs claimed the templates were stored on the device, that users cannot disable the feature, and that Samsung had “complete and exclusive control” over the data. They sued under Sections 15(a) and 15(b) of BIPA, alleging Samsung failed to publish a biometric data retention policy, failed to disclose that face templates were being created, and failed to obtain written consent. The district court dismissed, holding plaintiffs had not plausibly alleged that Samsung controlled or possessed the data.

Affirming, the Seventh Circuit held that BIPA’s operative terms—“possession,” “collect,” “capture,” and “obtain”—all require a private entity to have “control” over the biometric data. Even accepting that Samsung supplied devices and software used to create and store face templates that could be regulated by BIPA, the court found plaintiffs “allege[d] nothing from which we can reasonably infer that Samsung itself controlled the data.”

Siding with *Bhavilai* and likening the case to the Illinois Appellate Court’s decision in *Barnett*, the court reasoned that providing a tool capable of capturing biometric data is not the same as controlling the data itself. It illustrated the point with an analogy: a company that sells a camera lucida—a prism-based drawing tool—can be said to “capture” facial information when a user sketches a portrait, but the company does not thereby possess or control the resulting image. Applying that logic, the court found the complaint’s “primary deficiencies” were that plaintiffs never alleged that the data was stored anywhere but on their own devices, that Samsung forced the plaintiffs to photograph faces, or that Samsung could access, modify, or use the data. The court also rejected plaintiffs’ inference that face data travels to the Samsung Cloud along with backed-up photos, and found Samsung’s generic privacy-policy statement that it “may collect” biometrics too speculative to support plausible allegations of such collection by the Gallery app.¹

Ultimately, the court concluded: “Manufacturing a device (and installing related software) that allows a user to voluntarily take pictures of oneself, friends, family, and other passersby and, in the process, create face templates that remain parked within the confines of the user’s own personal device not only falls short of triggering BIPA’s statutory requirements but strays too far afield from the statute’s heartland.”

¹ Notably, the court assumed without deciding that the facial geometry data and face templates at issue are “biometric identifiers” or “biometric information” regulated by BIPA, so the decision does not address that issue.

Considerations for Businesses Operating in Illinois

Because BIPA only applies to private entities that “possess[],” “collect,” “capture,” or “otherwise obtain” biometric data, businesses have for years explored product designs that process and store biometric data locally on user devices rather than on company servers as a risk mitigation strategy. *G.T. v. Samsung* bolsters that approach, and its holding provides binding guidance for district courts in the Seventh Circuit. Where feasible, businesses offering products with biometric features in Illinois should continue to consider designs in which biometric data is created and stored only on the user’s device, no such data is transmitted to company or third-party servers, and the company retains no ability to access, modify, or use it. Designs that allow users to disable the biometric feature and delete the underlying data further mitigate BIPA risk.

Even where on-device processing supports a strong defense, businesses should continue to consider BIPA-compliant disclosures, consent mechanisms, and retention policies, where feasible, as additional risk mitigation strategies that complement on-device processing and storage.

Impact on Legal Arguments Available to Defendants in BIPA Cases

G.T. v. Samsung is notable for companies defending BIPA claims involving allegations that biometric data was processed or captured on the plaintiff’s device. Defendants in the Seventh Circuit can now cite published precedent establishing that BIPA does not reach biometric data that is processed and stored entirely on a device and where the defendant cannot access, modify, or use it. To overcome this defense at the pleading stage, plaintiffs must plausibly allege that the defendant actually accesses or has remote control over the biometric data at issue and support their allegations with specific facts. On this point, one aspect of *G.T. v. Samsung* that is particularly helpful to defendants is the Seventh Circuit’s rejection of the plaintiffs’ reliance on generic disclosures in Samsung’s privacy policy noting that Samsung “may collect” personal information “such as biometrics.” This language in the privacy policy was not specific enough to plausibly suggest “that the facial geometry data in question are actually gathered and saved by Samsung.”

The extent to which the decision in *G.T. v. Samsung* provides a path to dismissal or factual defenses to liability in other BIPA cases will depend on the plaintiff’s allegations and how the device or software at issue actually works. Where the allegations or underlying facts establish that biometric data is transmitted to company or third-party servers, or where the defendant retains access to it, defendants will likely need a different defense strategy.

While *G.T. v. Samsung* is only binding on federal courts within the Seventh Circuit, the decision is a meaningful development for BIPA defendants. It opens a potentially significant door to dismissal at the pleading stage or summary judgment in cases involving devices and software where biometric data is processed locally and remains stored on the user’s device.