UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

EMAD KASHKEESH and MICHAEL KOMORSKI, individually and on behalf of a class of similarly situated individuals,	)	21 C 3229
Plaintiffs,	)	Judge Gary Feinerman
vs.	)	
MICROSOFT CORPORATION,	)	
Defendant.	)	

MEMORANDUM OPINION AND ORDER

Emad Kashkeesh and Michael Komorski brought this putative class action in the Circuit Court of Cook County, Illinois, against Microsoft Corporation, alleging violations of the Illinois Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1 *et seq*. Doc. 1-1. Microsoft removed the suit to federal court, Doc. 1, and Plaintiffs move to remand two of their claims back to state court, Doc. 36. The motion is granted.

Background

Plaintiffs are former Uber drivers who worked primarily in Chicago. Doc. 28 at ¶¶ 32, 38. Upon registering as Uber drivers, each was required to submit his name, vehicle information, driver's license, and a profile picture to Uber through its mobile application. *Id*. ¶¶ 23, 32, 38. To gain access to Uber's platform and commence his driving duties, each had to photograph his face in real time through Uber's "Real Time ID Check" security feature. *Id*. at ¶¶ 33, 39. Unbeknownst to Plaintiffs, their pictures were transferred to Microsoft's Face Application Programming Interface ("Face API"), which is integrated into Uber's phone application as a security feature. *Id*. at ¶¶ 23-25. Microsoft's Face API collected and analyzed

Plaintiffs' facial biometrics to create a "geographic template" that it compared to the geographic template from the original profile picture to verify their identities. *Id*. at ¶¶ 25-26, 34, 40.

Microsoft never obtained Plaintiffs' written consent to capture, store, or disseminate their facial biometrics. *Id*. at ¶¶ 28, 35, 41. Microsoft also failed to make a publicly available policy regarding retention and deletion of their biometric information, and it profited from receiving that information. *Id*. at ¶¶ 29-30, 36, 42.

Discussion

"The party seeking removal has the burden of establishing federal jurisdiction, and federal courts should interpret the removal statute narrowly, resolving any doubt in favor of the plaintiff's choice of forum in state court." *Schur v. L.A. Weight Loss Ctrs., Inc.*, 577 F.3d 752, 758 (7th Cir. 2009). In an uncommon twist on a common theme, Plaintiffs argue that, in light of *Bryant v. Compass Group USA, Inc.*, 958 F.3d 617 (7th Cir. 2020), and *Thornley v. Clearview AI, Inc.*, 984 F.3d 1241 (7th Cir. 2021), they lack Article III standing to pursue in federal court their claims under Sections 15(a) and 15(c) of BIPA, 740 ILCS 14/15(a), (c), requiring the remand of those claims for want of subject matter jurisdiction. Microsoft responds that Plaintiffs have Article III standing because (1) their Section 15(a) claim alleges an "informational injury" sufficient to confer standing under the principles set forth in *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021), and (2) their Section 15(c) claim alleges the disclosure of private information sufficient to confer standing under the principles set forth in *TransUnion* and *Tims v. Black Horse Carriers, Inc.*, 184 N.E.3d 466 (Ill. App. 2021), *appeal allowed*, 184 N.E.3d 1029 (Ill. 2022).

A federal court has subject matter jurisdiction over a claim only if, among other things, the plaintiff has Article III standing to bring it. *See MAO-MSO Recovery II, LLC v. State Farm*

Mut. Auto. Ins. Co., 935 F.3d 573, 581 (7th Cir. 2019). "[T]he irreducible constitutional minimum of standing consists of three elements. [A] plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016) (citation and internal quotation marks omitted). "To establish injury in fact, a plaintiff must show that he or she suffered an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical." *Id*. at 339 (internal quotation marks omitted).

To be concrete, a plaintiff's injury "must be de facto; that is, it must actually exist," meaning that it must be "real" and not "abstract." *Ibid*. (internal quotation marks omitted). Both "tangible" and "intangible" injuries, even those that are "difficult to prove or measure," can be concrete. *Id*. at 341. Concreteness requires at least some "appreciable risk of harm" to the plaintiff. *Meyers v. Nicolet Rest. of De Pere, LLC*, 843 F.3d 724, 727 (7th Cir. 2016); *see also Spokeo*, 578 U.S. at 342 (holding that an injury is not concrete where the defendant's conduct does not "cause harm or present any material risk of harm"); *Gubala v. Time Warner Cable, Inc.*, 846 F.3d 909, 911 (7th Cir. 2017) (holding that the plaintiff lacked standing where he identified no "plausible (even if attenuated) risk of harm to himself").

I. Section 15(a) Claim

Section 15(a) of BIPA requires "[a] private entity in possession of biometric identifiers or biometric information" to "develop," "ma[k]e available to the public," and "comply with" "a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information" at certain junctures. 740 ILCS 14/15(a). In *Bryant*, the plaintiff alleged that the defendant, in violation of Section 15(a), collected and stored her biometric information—which

she provided when using the defendant's fingerprint-based vending machines—without making "publicly available a retention schedule and guidelines for permanently destroying the biometric identifiers and information it was collecting and storing." 958 F.3d at 619. *Bryant* held that the plaintiff lacked standing to bring that claim, reasoning that standing cannot rest on a mere violation of Section 15(a)'s publication duty. *See id*. at 626. The Seventh Circuit reaffirmed that holding in *Fox v. Dakkota Integrated Systems, LLC*, 980 F.3d 1146, 1154 (7th Cir. 2020). But *Fox* proceeded to hold that while "a mere failure to *publicly disclose* a data-retention policy" is insufficient to confer standing, a failure to "*comply with*" the policy under Section 15(a) is sufficient. *Id*. at 1154-55 (first emphasis added).

Like the plaintiff in *Bryant*, and unlike the plaintiff in *Fox*, Plaintiffs here allege only that Microsoft failed to disclose its retention and destruction policy, not that it failed to comply with that policy. Doc. 28 at ¶¶ 29, 36, 42, 56; Doc. 36 at 6. Under *Bryant* and *Fox*, it follows that Plaintiffs lack Article III standing to bring their Section 15(a) claim.

Pressing the contrary result, Microsoft argues that *TransUnion* undermined *Bryant*. Specifically, Microsoft contends that *TransUnion* "reaffirmed precedent"—*Federal Election Commission v. Akins*, 524 U.S. 11, 21 (1998), and *Public Citizen v. Department of Justice*, 491 U.S. 440, 449 (1989)—"holding that 'downstream consequences' are not required where, as here, the plaintiff allegedly 'fails to obtain information which must be publicly disclosure pursuant to a statute.'" Doc. 43 at 10 (quoting *Akins*, 524 U.S. at 21). But *Bryant* expressly considered and distinguished *Akins* and *Public Citizen* in ruling that a mere failure to comply with Section 15(a)'s disclosure duty does not give rise to Article III standing. *See Bryant*, 958 F.3d at 624-25. That *TransUnion* reaffirmed *Akins* and *Public Citizen* therefore has no impact, one way or the other, on the continued viability of *Bryant*.

Microsoft also contends that *TransUnion* made clear, contrary to *Bryant*, that an informational injury can support Article III standing where, as here, the plaintiff alleges "denial of information subject to public-disclosure or sunshine laws that entitle all members of the public to certain information." *TransUnion*, 141 S. Ct. at 2214; *see* Doc. 43 at 7. That contention fails to persuade. As an initial matter, *TransUnion* "d[id] not involve such a public-disclosure law," 141 S. Ct. at 2214, and thus cannot properly be read to implicitly overrule *Bryant*'s holding that the mere violation of such a law does not give rise to Article III standing. In any event, the Seventh Circuit adhered to *Bryant*'s holding in a post-*TransUnion* opinion that, in fact, cited *TransUnion*. *See Cothron v. White Castle Sys., Inc.*, 20 F.4th 1156, 1161 (7th Cir. 2021) (holding that a plaintiff alleging a Section 15(d) violation suffered Article III injury, and reasoning that "Section 15(d) is … unlike other sections of [BIPA] that impose duties owed only to the public generally—the violation of which does not, without more, confer standing.") (citing *Bryant*, 958 F.3d at 626, for the proposition that "a violation of section 15(a)'s duty to provide a data-retention schedule to the public does not inflict an Article III injury"). From the perspective of a federal district court, *Cothron* defeats Microsoft's submission that *TransUnion* fatally undermines *Bryant*.

Accordingly, Plaintiffs lack Article III standing to pursue their Section 15(a) claim.

II. Section 15(c) Claim

Section 15(c) of BIPA prohibits private entities in possession of biometric information from "sell[ing], leas[ing], trad[ing], or otherwise profiting from a person's or customer's biometric … information." 740 ILCS 14/15(c). In *Thornley*, the plaintiffs alleged that the defendant violated Section 15(c) by harvesting their biometric information, placing it on a database, and offering it for sale. *See* 984 F.3d at 1243. As *Thornley* understood it, Section

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.