

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

CHARLENE FIGUEROA and JERMAINE BURTON,)	
individually and on behalf of all others similarly situated,)	
)	19 C 1306
Plaintiffs,)	
)	Judge Gary Feinerman
vs.)	
)	
KRONOS INCORPORATED,)	
)	
Defendant.)	

MEMORANDUM OPINION AND ORDER

Charlene Figueroa and Jermaine Burton brought this putative class action in the Circuit Court of Cook County, Illinois, against Kronos, Inc., alleging violations of the Illinois Biometric Information Privacy Act (“BIPA”), 740 ILCS 14/1 *et seq.* Doc. 1-1. Kronos timely removed the suit under 28 U.S.C. § 1453(b), premising jurisdiction on the Class Action Fairness Act, 28 U.S.C. § 1332(d). Doc. 1. Kronos moved under Civil Rule 12(b)(6) to dismiss the complaint and, in the alternative, under Civil Rules 23(c)(1)(A) and 23(d)(1)(D) to strike its class allegations. Docs. 29, 32. The court denied both motions and, having held that Plaintiffs had standing to pursue claims under Sections 15(b) and 15(d) of BIPA, ordered supplemental briefing regarding their standing to pursue a claim under Section 15(a). Doc. 128 (reported at __ F. Supp. 3d __, 2020 WL 1848206 (N.D. Ill. Apr. 13, 2020)). The court concludes that it lacks jurisdiction over Plaintiffs’ Section 15(a) claim.

Background

Although the parties agree that the court has jurisdiction over Plaintiffs’ Section 15(a) claims, standing is a jurisdictional defect that the court must “police ... *sua sponte.*” *Hay v. Ind. State Bd. of Tax Comm’rs*, 312 F.3d 876, 879 (7th Cir. 2002); *see also Carrol v. Stryker Corp.*,

658 F.3d 675, 680 (7th Cir. 2011) (“Although neither the parties nor the district court addressed subject-matter jurisdiction, we have an independent obligation to satisfy ourselves that jurisdiction is secure before proceeding to the merits.”). In fulfilling that responsibility, the court “properly may look beyond the factual allegations of the complaint,” *Hay*, 312 F.3d at 879, though here the complaint alone shows that the court lacks jurisdiction. The complaint’s factual allegations are detailed in the court’s earlier opinion, familiarity with which is assumed. The facts pertinent to the Section 15(a) standing issue are reiterated here.

Kronos is a company that, among other things, provides Illinois employers with biometric-based time clocks that require employees to use their biometric information to punch in and out of work. Doc. 1-1 at ¶¶ 1-2. When beginning work for an employer that uses such a device, an employee must have her fingerprint or palm print scanned to enroll in the Kronos database. *Id.* at ¶ 25. Kronos does not inform those employees that it is collecting, storing, or using their biometric data, nor does Kronos inform them of the purposes for collecting their data or to whom the data will be disclosed. *Id.* at ¶¶ 26-27. Kronos does not maintain retention schedules or guidelines for permanently destroying the data. *Id.* at ¶¶ 28, 32. Kronos has not destroyed biometric data when the initial purpose for obtaining it has been satisfied or within three years of an employee’s last interaction with her employer. *Id.* at ¶ 32. Employees are not told whether and to whom Kronos discloses their data or what would happen to the data in the event of a Kronos merger or bankruptcy. *Id.* at ¶ 33.

Figuroa worked as an hourly employee at Tony’s Finer Food Enterprises Inc. from March 2017 through September 2018. *Id.* at ¶ 35. Burton worked for BWAY from January 2017 through April 2017. *Id.* at ¶ 49. Both were required, as a condition of their employment, to scan their fingerprints using a Kronos timekeeping device. *Id.* at ¶¶ 35, 49.

Kronos stored Plaintiffs' fingerprint data in its database or databases. *Id.* at ¶¶ 36, 50. At no point were Plaintiffs informed of the purposes or length of time for which Kronos was collecting, storing, using, or disseminating their data. *Id.* at ¶¶ 39, 52, 80. Nor were Plaintiffs informed of any biometric data retention policy developed by Kronos or whether it would ever permanently delete their data. *Id.* at ¶¶ 40, 53, 81. That is because Kronos lacked such a policy when Plaintiffs were hired, *id.* at ¶¶ 28, 81, which means that it failed to adhere to or publish such a policy at that time, *id.* at ¶¶ 73-74—though “years later” it implemented and published a policy, “long after being sued in other BIPA actions,” Doc. 50 at 14-15.

At no point did Plaintiffs receive or sign a release allowing Kronos to collect, store, use, or disseminate their biometric data. Doc. 1-1 at ¶¶ 41, 54. Nonetheless, Kronos disseminated their data to other firms, including firms hosting the data in data centers. *Id.* at ¶¶ 45, 79. Plaintiffs would not have provided their data to Kronos had they known it would retain the data for an indefinite time period without their consent. *Id.* at ¶¶ 43, 56.

Discussion

BIPA “regulat[es] the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.” 740 ILCS 14/5(g). “Biometric identifier” is defined to include a “fingerprint.” 740 ILCS 14/10. A biometric identifier is particularly sensitive because, unlike a social security number, it cannot be “changed,” which means that “once [it is] compromised, the individual has no recourse[and] is at heightened risk for identity theft.” 740 ILCS 14/5(c). Recognizing this concern, Illinois adopted BIPA to protect the privacy of biometric data. *See Rosenbach v. Six Flags Entm’t Corp.*, 129 N.E.3d 1197, 1206-07 (Ill. 2019). BIPA allows a private right of action by “[a]ny person aggrieved by a violation.” 740 ILCS 14/20.

At issue here is Plaintiffs' standing to bring their claim under Section 15(a), which requires private entities that possess biometric data to develop, publish, and comply with a written policy that includes a retention schedule and destruction guidelines. 740 ILCS 14/15(a). A federal court has subject matter jurisdiction over a claim only if the plaintiffs have 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*, 136 S. Ct. 1540, 1547 (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 1548 (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 1549. 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*, 136 S. Ct. at 1550 (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").

The Seventh Circuit in *Bryant v. Compass Group USA, Inc.*, 958 F.3d 617 (7th Cir. 2020), applied these principles to BIPA claims. There, the plaintiff alleged that the defendant

collected and stored her biometric information when she used the defendant's fingerprint-based vending machines in her employer's cafeteria. *Id.* at 619. She claimed that the defendant violated Section 15(a) by doing so without making "publicly available a retention schedule and guidelines for permanently destroying the biometric identifiers and information it was collecting and storing." *Ibid.* She further claimed that the defendant violated Section 15(b)—which provides that, in order to disclose or otherwise disseminate a person's biometric data, a private entity must (with limited exceptions) make certain disclosures to the person and obtain the person's consent, 740 ILCS 14/15(b)—by failing to provide the required disclosures or obtain her written consent. *Bryant*, 958 F.3d at 619.

The Seventh Circuit concluded that the plaintiff had standing to bring the Section 15(b) claim. *See id.* at 623-24. First, applying the framework Justice Thomas offered in his *Spokeo* concurrence, the court held that the plaintiff's allegation that the defendant collected her personal biometric information without her consent "assert[ed] a violation of her own rights," as distinct from "seek[ing] to vindicate public rights." *Id.* at 624 (citing *Spokeo*, 136 S. Ct. at 1551-52 (Thomas, J., concurring)). Second, the court reasoned—as this court did in its prior opinion, 2020 WL 1848206, at *3—that the plaintiff suffered an "informational injury" sufficient to confer standing because the defendant had "withheld substantive information to which [she] was entitled and thereby deprived her of the ability to give the *informed* consent section 15(b) mandates." *Bryant*, 958 F.3d at 626. By contrast, the court held that the plaintiff lacked standing for the Section 15(a) claim because the defendant's obligation to publicize a data retention schedule and destruction guidelines "is owed to the public generally, not to particular persons whose biometric information the entity collects," and the plaintiff "allege[d] no particularized harm that resulted from [the defendant's] violation of section 15(a)." *Ibid.*

As both parties observe, Doc. 137 at 5-6; Doc. 138 at 2-3, Section 15(a) requires a covered entity not only to publish a retention and destruction policy, but also to adhere to it. *Bryant* straightforwardly holds that standing cannot rest on a mere violation of the publication duty. As in *Bryant*, Plaintiffs here do not allege that Kronos's failure to publicize its retention policy injured them. Nor could they have, since they allege that because of Kronos's violations of Sections 15(b) and (d), "most employees don't know they are interacting with Kronos when they have their biometrics scanned by their employer's Kronos devices, let alone providing it their biometric data," and therefore would "have no reason to affirmatively seek out Kronos' website and search for its biometric data policies." Doc. 1-1 at ¶ 28. If Plaintiffs would never have sought out a biometric data policy published by Kronos, they cannot have suffered any concrete injury due to its failure to develop and publish such a policy.

While Plaintiffs appear to accept that result—relying instead on Section 15(a)'s destruction prong for standing, of which more in a moment—Kronos contends that Plaintiffs allege a "particularized harm" stemming from its alleged violation of its publication duty. Doc. 137 at 2-3, 6-7. According to Kronos, "the Complaint alleges that Plaintiffs would have changed their behavior had they known of the information required by Section 15(a)." Doc. 137 at 2. That is correct but misses the critical point—Section 15(a) does not obligate Kronos to inform specific individuals like Plaintiffs of its policy. *See Bryant*, 958 F.3d at 626 ("[T]he duty to disclose under section 15(a) is owed to the public generally, not to particular persons whose biometric information the entity collects."). Without knowing that Kronos was collecting or storing their biometric information, Plaintiffs would "have [had] no reason to affirmatively seek out Kronos' website and search for its biometric data policies" even if those policies had been publicly available. Doc. 1-1 at ¶ 28.

Kronos also argues that other portions of the complaint suggest that Plaintiffs were in fact aware that it was storing their information—but, as shown above, the complaint clearly alleges the contrary. *Ibid.* (“[M]ost employees don’t know they are interacting with Kronos when they have their biometrics scanned by their employer’s Kronos devices, let alone providing it their biometric data.”). The mere fact that Plaintiffs used Kronos machines does not mean they knew that Kronos collected and stored their biometric information. Plaintiffs accordingly cannot show that Kronos’s alleged violation of its publication duty caused them *any* injury, let alone the injury in fact required for Article III standing.

Kronos’s alleged violation of Section 15(a)’s destruction duty presents a closer question, but it nonetheless fails to confer standing for the 15(a) claim. In *Gubala v. Time Warner Cable, Inc.*, the plaintiff alleged that the defendant violated a subsection of the Cable Communications Policy Act, 47 U.S.C. § 551(e), by failing to destroy personally identifiable consumer information once retention was no longer necessary for the purpose for which the data was collected. 846 F.3d at 910. But even though the defendant’s retention of data “unquestionably” presented some “*risk of harm*” to the plaintiff, the Seventh Circuit held that the plaintiff lacked standing because he did not allege the defendant had “ever given away or leaked or lost any of his personal information[,] ... intend[ed] to give it away[,] or [wa]s at risk of having the information stolen from it.” *Id.* at 910. As Plaintiffs put it, *Gubala* “held that mere retention of information by an entity that has come by it legally does not confer Article III standing.” Doc. 138 at 3. Here, Kronos’s alleged failure to follow retention and destruction guidelines presents a similarly bare risk of harm and cannot establish standing without a particularized allegation that such retention poses a real risk of harm to Plaintiffs.

Plaintiffs' efforts to distinguish *Gubala* are unpersuasive. First, Plaintiffs argue that Kronos's obligation to abide by a destruction policy reflects, in Justice Thomas's typology from *Spokeo*, a private right owed to those whose information Kronos holds. Doc. 138 at 2-3. But that reasoning would have applied with equal force in *Gubala*, where the defendant was under a statutory duty to destroy the plaintiff's personal information, and the Seventh Circuit did not purport to overturn *Gubala* in *Bryant*.

Second, Plaintiffs observe that *Gubala* involved the *lawful* collection of personal information, while they allege that Kronos violated BIPA and therefore *unlawfully* collected their biometric information. *Id.* at 3. *Gubala*'s reasoning, however, does not turn on whether or not the defendant lawfully acquired the information at issue. To be sure, the retention of biometric information by an entity that clandestinely or maliciously acquired it may suggest a higher risk of further dissemination or exposure. But nothing here suggests that Kronos's alleged failure to comply with BIPA's formal requirements made it an especially risky information holder.

Third, Plaintiffs argue that Kronos's alleged dissemination of their biometric information shows that the risk absent in *Gubala* is present here. *Id.* at 3. But the only entities to which Kronos allegedly disseminated Plaintiffs' information are the firms hosting their data in data centers. Doc. 1-1 at ¶¶ 45, 79. Even if such routine *dissemination* violates BIPA and is itself an injury in fact under Section 15(b), it does not present the real risk of further harm required by *Gubala* to also render the *retention* of data under Section 15(a) an injury in fact. Plaintiffs do not explain how Kronos's dissemination of their biometric information transforms its failure to follow a retention and destruction policy into a concrete injury.

Finally, Plaintiffs contend that biometric information's unchangeable and sensitive nature distinguishes it from other types of personal information. Doc. 138 at 3-4. In their view, a risk

that would be insufficient to confer standing for a plaintiff alleging the improper retention of ordinary personal information may suffice for the improper retention of biometric information. But Plaintiffs cite no authority for the proposition that an especially grave harm can suffice for standing even where the probability of its occurrence is slight. Indeed, *Gubala* focused exclusively on the plaintiff's failure to allege a real risk of disclosure—not on the magnitude of the consequences that could flow from disclosure. As in *Gubala*, Plaintiffs do not allege a sufficiently concrete risk that their information could be leaked or disclosed as a result of Kronos's wrongful retention thereof. Even if the consequences of disclosure would be graver here, that does not remove this case from *Gubala*'s reach.

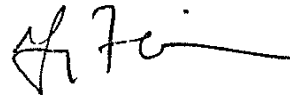
For its part, Kronos adds one more argument for standing: that Plaintiffs allege that they suffered mental anguish over whether it would ever delete their biometric data. Doc. 137 at 3-4, 8. But *Gubala* squarely instructs against finding standing on that basis. *See Gubala*, 846 F.3d at 911 (holding that the plaintiff lacked standing where “[a]ll he[was] left with [wa]s a claim that the violation ... ha[d] made him *feel* aggrieved”).

Conclusion

The court lacks subject matter jurisdiction over Plaintiffs' Section 15(a) claim. When a case is filed in state court and removed to federal court, and when the federal court finds that it lacks subject matter jurisdiction, the appropriate disposition (with narrow exceptions not pertinent here) is a remand to state court under 28 U.S.C. § 1447(c). *See Collier v. SP Plus Corp.*, 889 F.3d 894, 897 (7th Cir. 2018) (“[Section] 1447(c) required the district court to remand this case to state court, because it does not satisfy Article III's requirements.”). Where, as here, the court lacks jurisdiction only over a portion of a suit, it should remand only that portion. *See Bergquist v. Mann Bracken, LLP*, 592 F.3d 816, 819 (7th Cir. 2010) (“Federal law

does not permit a district judge to remand the complete litigation just because portions belong in state court. ... If some parts of a single suit are within federal jurisdiction, while others are not, then the federal court must resolve the elements within federal jurisdiction and remand the rest—unless the balance can be handled under the supplemental jurisdiction.”). Accordingly, Plaintiffs’ Section 15(a) claim is severed under Civil Rule 21 from the rest of the suit and remanded to state court. *See Gaffney v. Riverboat Servs. of Ind., Inc.*, 451 F.3d 424, 443-44 (7th Cir. 2006) (approving severance where “[t]he validity of the claims before us does not depend, as a matter of law, on the outcome of the severed claims”); *Hebel v. Ebersole*, 543 F.2d 14, 17 (7th Cir. 1976) (approving severance of “logically separable” claims).

July 24, 2020



United States District Judge