UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

STEVEN VANCE and TIM JANECYK, for themselves and others similarly situated,	)	
Plaintiffs,	)	
v.	)	20 C 577
INTERNATIONAL BUSINESS MACHINES CORPORATION, a New York corporation,	)	
Defendant.	)	

MEMORANDUM OPINION

CHARLES P. KOCORAS, District Judge:

Before the Court is Defendant International Business Machines Corporation's ("IBM") motion to dismiss Plaintiffs Steven Vance ("Vance") and Tim Janecyk's ("Janecyk") (collectively, "Plaintiffs") Second Amended Class Action Complaint ("SAC") under Federal Rule of Civil Procedure 12(b)(6). For the following reasons, the Court will grant the motion in part.

BACKGROUND

For purposes of this motion, the Court accepts as true the following facts from the complaint. *Alam v. Miller Brewing Co.*, 709 F.3d 662, 665–66 (7th Cir. 2013). All reasonable inferences are drawn in Plaintiffs' favor. *League of Women Voters of Chicago v. City of Chicago*, 757 F.3d 722, 724 (7th Cir. 2014).

Plaintiffs Vance and Janecyk are both Illinois residents. Defendant IBM is a multinational technology corporation organized under the laws of the State of New York with a corporate headquarters in Armonk, New York.

Vance has had an account with Flickr, a photo sharing service, since 2006. In 2008, Vance uploaded a photo of himself and two family members to Flickr from his computer in Illinois. Similarly, Janecyk has had a Flickr account since 2008 and uploaded a photo of himself to Flickr in 2011. Yahoo!, Flickr's parent company at the time, subsequently made Vance's photo available to IBM in 2014 when it released over 99 million photos in a single, downloadable dataset called YFCC100M ("Flickr Dataset").

Plaintiffs allege that IBM used the Flickr Dataset to create its own dataset (the "IBM Dataset"). The IBM Dataset was allegedly comprised of over one million front-facing images of human faces. In each image, IBM allegedly extracted 68 key-points and at least ten facial coding schemes, such as craniofacial distances, craniofacial areas, craniofacial ratios, facial symmetry, facial regions contrast, skin color, age prediction, gender prediction, subjective annotation, and pose and resolution.

Plaintiffs allege that IBM subsequently disseminated a dataset created from information extracted from the IBM Dataset. IBM called this dataset "Diversity in Faces" ("DIF Dataset"). Each image in the DIF Dataset could allegedly be traced back to the individual Flickr account to which it was originally uploaded.

Based on these facts, Plaintiffs filed the instant class action complaint on March 12, 2020. Plaintiffs allege that IBM did not establish a publicly available retention schedule and guidelines for destroying biometric information in violation of Section 15(a) of the Illinois Biometric Information Privacy Act, 740 ILCS § 14/1 et seq. ("BIPA") (Count One); IBM collected, captured, or otherwise obtained Plaintiffs' biometric information without written informed consent in violation of BIPA Section 15(b) (Count Two); IBM sold Plaintiffs' biometric information in violation of BIPA Section 15(c) (Count Three); IBM disclosed or otherwise disseminated Plaintiffs' biometric information without Plaintiffs' consent or required by law in violation of BIPA Section 15(d) (Count Four); IBM failed to use reasonable care to protect Plaintiffs' biometric information from disclosure and did not store Plaintiffs' biometric information in a matter the same as IBM would store other confidential information in violation of BIPA Section 15(e) (Count Five); a state law unjust enrichment claim (Count Six); and a state law injunctive relief claim (Count Seven).[1]

Plaintiffs seek statutory damages of $5,000 for each willful and reckless violation and $1,000 for each negligent violation of BIPA. IBM moved to dismiss the complaint under Rule 12(b)(6) on April 16, 2020.

[1] Count Seven was improperly labeled as Count Six.

LEGAL STANDARD

A motion to dismiss under Federal Rule of Civil Procedure 12(b)(6) "tests the sufficiency of the complaint, not the merits of the case." *McReynolds v. Merrill Lynch & Co.*, 694 F.3d 873, 878 (7th Cir. 2012). The allegations in the complaint must set forth a "short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). A plaintiff need not provide detailed factual allegations, but it must provide enough factual support to raise its right to relief above a speculative level. *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2007).

A claim must be facially plausible, meaning that the pleadings must "allow . . . the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). The claim must be described "in sufficient detail to give the defendant 'fair notice of what the . . . claim is and the grounds upon which it rests.'" *E.E.O.C. v. Concentra Health Servs., Inc.*, 496 F.3d 773, 776 (7th Cir. 2007) (quoting *Twombly*, 550 U.S. at 555). "[T]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements," are insufficient to withstand a 12(b)(6) motion to dismiss. *Iqbal*, 556 U.S. at 678.

DISCUSSION

As a preliminary matter, we note that the Seventh Circuit's recent decision in *Bryant v. Compass Group USA Inc*., brings into question our subject-matter jurisdiction over Plaintiffs' claims under BIPA Section 15(a). 958 F.3d 617 (7th Cir. 2020). In *Bryant*, the Seventh Circuit resolved an important issue that has divided courts in our

District for the past three years: what BIPA violations are sufficiently substantive to qualify as an injury for purposes of standing under Article III of the U.S. Constitution ("Article III").

Applying Justice Thomas's rubric from his concurrence in *Spokeo Inc., v. Robbins*, 136 S. Ct. 1540, 1551 (2016), the *Bryant* Court distinguished between the duty owed under BIPA Section 15(b)—requiring that private entities obtain informed consent to collect biometric information—and that owed under Section 15(a), requiring private entities to make publicly available a data retention schedule and guidelines for permanently destroying collected biometric identifiers and information. 958 F.3d at 624.

The *Bryant* Court found that the obligations under the former are owed to private individuals, and therefore, a violation of BIPA Section 15(b) invades a plaintiff's personal privacy right to consider the terms under which her biometric information is collected and used. *Id.* In contrast, the obligations under BIPA Section 15(a) are owed to the public generally. *Id.* at 626. Therefore, a violation of that Section does not invade a plaintiff's personal privacy rights in a concrete manner. *Id.* Accordingly, the *Bryant* Court held that a violation of Section BIPA Section 15(b) is a substantive violation that creates a concrete and particularized Article III injury, whereas a violation of BIPA Section 15(a) is procedural and does not create such an injury. *Id.*

Applying the *Bryant* Court's holding, we conclude that we lack subject-matter jurisdiction over Plaintiffs' Section 15(a) claims. In their complaint, Plaintiffs allege

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.