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

MARK MARTELL, on behalf of himself and all others similarly situated,	
Plaintiff,	Case No. 23 C 5449
v.	Honorable Sunil R. Harjani
X CORP.,	
Defendant.	

MEMORANDUM OPINION AND ORDER

In this lawsuit, Plaintiff Mark Martell brings a Class Action Complaint on behalf of himself and others similarly situated for violations of the Illinois Biometric Information Privacy Act (BIPA) against Defendant X Corp.[1] Martell alleges that he uploaded a photograph of himself on the social media platform X (formerly known as Twitter), which X analyzed for nudity and other not-safe-for-work content using a Microsoft product called PhotoDNA. Plaintiff alleges that PhotoDNA created a unique digital signature of the photograph, known as a "hash", to compare against other photographs' hashes. As a result, Plaintiff alleges that creating this hash necessarily created a scan of his facial geometry in violation of BIPA. Defendant moved to dismiss the Complaint pursuant to Federal Rule of Civil Procedure 12(b)(6), claiming that the Complaint fails to state a claim upon which relief can be granted. For the reasons stated below, Defendant's motion [15] is granted.

Legal Standard

"A motion under Rule 12(b)(6) tests whether the complaint states a claim on which relief may be granted." *Richards v. Mitcheff*, 696 F.3d 635, 637 (7th Cir. 2012). To survive a Rule 12(b)(6) motion, "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). This pleading standard does not necessarily require a complaint to contain detailed factual allegations. *Twombly*, 550 U.S. at 555. Rather, "[a] claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Adams v. City of Indianapolis*, 742 F.3d 720, 728 (7th Cir. 2014) (quoting *Iqbal*, 556 U.S. at 678). When deciding a motion to dismiss under Rule 12(b)(6), the court accepts as true all factual allegations in the complaint and draws all inferences in favor of the plaintiff. *Heredia v. Capital Management*

---

[1] Defendant X Corp. is the successor organization to Twitter, Inc.

Services, L.P., 942 F.3d 811, 814 (7th Cir. 2019). However, a complaint must consist of more than "threadbare recitals of the elements of a cause of action, supported by mere conclusory statements." *Iqbal*, 556 U.S. at 678 (quoting *Twombly*, 550 U.S. at 555).

Discussion

The Defendant raises three primary issues with the Complaint. First, Defendant argues the Complaint should be dismissed because Plaintiff fails to plausibly allege that PhotoDNA collects facial geometry scans as defined by BIPA. Second, Defendant contends that the hashes created by PhotoDNA are not biometric information or biometric identifiers under BIPA because they cannot be used to identify a person. Finally, Defendant argues that the Communication Decency Act bars Plaintiff's claim.[2] The Court will address each of these arguments in turn.

Initially, it is important to understand what BIPA protects. In 2008, the Illinois legislature found that businesses were increasingly using biometrics to streamline financial transactions and security screenings. The legislature found that biometrics—unlike other identifiers such as social security numbers that can be changed if compromised—are "biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." 740 ILCS 14/5(c). The legislature also found that an overwhelming majority of the public was weary of using biometrics when such information was tied to finances and other personal information. Since the full ramifications of biometric technology were not fully known, the legislature found that "public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information." 740 ILCS 14/5(g).

BIPA prohibits private entities from collecting or capturing "a person's or a customer's biometric identifier or biometric information" without first providing written notice that the information is being collected and of the specific purpose and length of the term for the collection, storage, and use of the data. 740 ILCS 14/15(b). The entity must then receive written consent from the subject of the biometric identifier or biometric information. *Id.* BIPA defines "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10. BIPA further defines "biometric information" as any information "based on an individual's biometric identifier used to identify an individual." *Id.*

Facial Geometry

Defendant first argues that the Complaint should be dismissed because Plaintiff fails to plausibly allege that PhotoDNA collects facial geometry scans as defined by BIPA. Defendant contends that according to Microsoft's website, which Plaintiff cited in the Complaint, PhotoDNA

---

[2] In the alternative, Defendant argues that the Court should dismiss Plaintiff's Section 15(d) claim and his claim for enhanced statutory damages. The Court does not reach these arguments, because the Complaint was dismissed on other grounds.

2

is not facial recognition software and cannot be used to identify a person, so it cannot be a scan of facial geometry. Defendant argues that an allegation that PhotoDNA scanned the facial geometry of the individuals in the photograph is required for the scans to be considered a biometric under BIPA. Plaintiff responds that he sufficiently alleged that PhotoDNA scans for facial geometry.

Whether PhotoDNA scans for facial geometry is an important consideration because a scan of face geometry is required for the conduct to be covered by BIPA. BIPA defines "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10. The statute then goes on to list items that do not qualify as biometric identifiers including writing samples, written signatures, demographic data, tattoo descriptions, physical descriptions, and relevant to this dispute, photographs. *Id.* Thus, Plaintiff must allege that the PhotoDNA scanned individuals' face geometry and not just that it scanned a photo. This consideration also impacts what qualifies as biometric information because biometric information is "based on an individual's biometric identifier," so if PhotoDNA only scans a photograph, it is not biometric information.

Plaintiff responds that he sufficiently alleged that the PhotoDNA software collected facial geometry scans when it created the unique hash for the photograph. Specifically, Plaintiff alleged that "PhotoDNA creates a unique digital signature (known as a 'hash') of an image which is then compared against signatures (hashes) of other photos to find copies of the same image." Compl. [1-2] ¶ 25. Plaintiff included in the Complaint an image from Microsoft's website, which he alleged shows that PhotoDNA creates "a unique digital signature, or 'hash,' from any image containing a person's face [which] necessitates creating a scan of that person's facial geometry." *Id.* ¶ 27. The Court finds that these allegations are conclusory. The fact that PhotoDNA creates a unique hash for each photo does not necessarily imply that it is scanning for an individual's facial geometry when creating the hash.

The absence of factual allegations to this point is evident when Plaintiff's allegations are compared to BIPA complaints where district courts found that a plaintiff plausibly alleged that the defendant collected their biometric identifier. For example, in *Carpenter v. McDonald's Corp.*, the plaintiff alleged that the defendant's "AI voice assistant is able to extract voice information including pitch, volume, and duration along with identifying information like age, gender, nationality, and national origin." 580 F. Supp. 3d 512, 517 (N.D. Ill. 2022). The plaintiff also alleged that the AI voice assistant used an acoustic model that was trained to receive "a graphical representation, measurement, or illustration of acoustic patterns." *Id.* The court also noted that "importantly, Plaintiff alleges that McDonald's uses the AI and data to actually identify unique individuals." *Id.* The court found that these allegations were sufficient to plausibly allege that the technology "mechanically analyzes customers' voices in a measurable way such that McDonald's has collected a voiceprint[.]" *Id.* Here, Plaintiff has not made similar factual allegations but instead merely concludes that creating the digital hash "necessitates creating a scan of that person's facial geometry." Compl. [1-2] ¶ 27. Plaintiff's Complaint does not include factual allegations about the hashes including that it conducts a face geometry scan of individuals in the photo. Allegations that

3

a photo was scanned are insufficient to plausibly allege that PhotoDNA creates a scan of an individual's face geometry under BIPA.

Similarly, in *Rivera v. Google Inc.*, the plaintiff alleged that when she was photographed on a Google Android device, those photos were automatically uploaded to Google Photos and Google immediately scanned each of the photos. 238 F. Supp. 3d 1088, 1091 (N.D. Ill. 2017). The plaintiff alleged that the scans "located her face and zeroed in on its unique contours to create a 'template' that maps and records her distinct facial measurements." *Id.* The court found that the allegation that Google created a biology-based face template of the individuals in the photos was sufficient to allege a scan of face geometry under BIPA. *Id.* at 1095. Importantly, the court noted that the plaintiff was not alleging that the photos themselves were biometric identifiers, but rather that the face templates were biometric identifiers. *Id.* at 1096. Here, Plaintiff has not made that distinction. While Plaintiff alleged that PhotoDNA scanned the photo to create a unique hash, Plaintiff did not allege facts indicating that the hash is a scan of face geometry, as opposed to merely a record of the photo. Plaintiff's allegations leave open the question of whether the hash is a unique representation of the entire photo or specific to the faces of the people in the picture. If the scan merely compares the image to see if it is the same as other images, that does not imply the use of facial geometry. If, instead, PhotoDNA identifies and scans the facial geometry of individuals in the photos and the hash saves those facial geometry scans, then it could be a biometric identifier under BIPA. But Plaintiff does not allege that the hash process takes a scan of face geometry, rather he summarily concludes that it must. The Court cannot accept such conclusions as facts adequate to state a plausible claim.

Biometric Identifiers and Biometric Information

Defendant next argues that Plaintiff failed to allege a viable BIPA claim because the Complaint does not allege that PhotoDNA could be used to identify the individuals in the photos. Defendant argues that biometric information must be used to identify an individual because, as defined by the statute, BIPA biometric information is any information "based on an individual's biometric identifier *used to identify an individual*." 740 ILCS 14/10 (emphasis added). Plaintiff does not dispute that this is required under the definition of biometric information and instead argues that the PhotoDNA hashes qualify as "biometric identifiers" and further that BIPA does not require that biometric identifiers be used to identify an individual because, unlike the definition for biometric information, the definition for biometric identifier does not include the 'used to identify an individual' language.

While Plaintiff is correct that the definition of biometric identifier does not include the phrase 'used to identify an individual,' the term itself includes the word identifier. As defined by BIPA "'Biometric identifier' means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10. When analyzing the plain language of the statute, a court in this district found that this was a specific and complete list where each item was "a biology-based set of measurements ('biometric') that can be used to identify a person ('identifier')." *Rivera*, 238 F. Supp. 3d at 1094. Further, Merriam-Webster defines "identifier" as "one that identifies" and

4

Black's Law Dictionary defines "identify" as "to prove the identity of (a person or thing)." Merriam-Webster's Unabridged Dictionary; Black's Law Dictionary (11th ed. 2019). Beyond that, if the Court were to read BIPA as applying to any retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry without those items actually identifying an individual, it would contravene the very purpose of BIPA. If a face geometry scan could not identify an individual, how could a business provide the individual with notice and obtain their consent? BIPA requires that before a private entity can collect "a person's or a customer's biometric identifier," it must inform "the subject" that the information is being collected and receive "a written release executed by the subject of the biometric identifier[.]" 740 ILCS 14/15. Thus, under a plain reading of BIPA, Plaintiff must allege that the biometric identifier can be used to identify an individual.

Plaintiff points to cases where courts found that other kinds of technology that scanned an individual's face geometry were a biometric identifier and argues that BIPA does not require him to allege that biometric identifiers are used to identify an individual. For example, Plaintiff relies on *Sosa v. Onfido, Inc.*, to support his argument that the hashes should be considered biometric identifiers. 600 F. Supp. 3d 859 (N.D. Ill. 2022). In *Sosa*, the plaintiff alleged that after defendant's software scans an individual's identification and photograph to locate the facial image in each document, it extracts a "faceprint"—a unique numerical representation of the shape or geometry of each facial image—which it then compares to the consumer's identification and photograph, after which it generates a score based on the similarity of the faceprints. *Id.* at 865. The court found that as alleged, the software "scans identification cards and photographs to locate facial images and extracts a unique numerical representation of the shape or geometry of each facial image" which plausibly constituted a scan of face geometry. *Id.* at 871. Plaintiff has made no such allegations about PhotoDNA scanning the faces in photos uploaded on Twitter. Plaintiff only alleges that the photo was scanned, without alleging that the faces in the photo were scanned to identify an individual. Without allegations that PhotoDNA uses facial geometry to identify individuals, Plaintiff failed to allege that the hashes are biometric identifiers.

Plaintiff further relies on *American Civil Liberties Union v. Clearview AI, Inc.*, to support his argument that PhotoDNA's hashes should be considered facial scans. 2021 WL 4164452 (Ill. Cir. Ct. Aug. 27, 2021). However, as with *Sosa*, the allegations in *Clearview* are distinguishable from the facts Plaintiff alleges in the Complaint. In *Clearview*, when the system scanned a photo, it measured and recorded data such as the shape of the cheekbones and the distance between eyes, nose, and ears, and assigned that data a numerical value, which it then used to identify someone in other photos. *Id.* at *1. The court held that BIPA applied to such faceprints. *Id.* at *5. Here, Plaintiff does not allege that any details of an individual's face are measured or recorded during the PhotoDNA scan or that those records were used to identify individuals.

The fatal flaw in Plaintiff's Complaint is that he failed to allege that any type of facial scan occurs during the hash creation process. Without that, there can be no scan of face geometry which could be used to identify an individual, as is required to be considered a biometric identifier under BIPA. True, the cases Plaintiff cites all stand for the proposition that BIPA allows for face geometry scans to be created from photographs. *Sosa*, 600 F. Supp. 3d at 873 ("In conclusion, we

5

join the Illinois courts that have uniformly rejected the argument that BIPA exempts biometric data extracted from photographs.") (internal citation and quotation omitted); *Clearview*, 2021 WL 4164452, at *5 (rejecting the argument that BIPA does not apply to faceprints derived from photographs).[3] But that principle alone does not save his Complaint because it fails to sufficiently allege that the PhotoDNA hashes consist of a scan of face geometry that could be used to identify an individual. Contrary to Plaintiff's arguments, courts have routinely held that a biometric identifier is "a biology-based set of measurements ('biometric') that can be used to identify a person ('identifier')." *Rivera*, 238 F. Supp. 3d at 1094.[4] As such, Plaintiff fails to sufficiently allege a BIPA claim and the Complaint is dismissed.

The Communication Decency Act

Since the Court will provide Plaintiff with leave to file an amended complaint (if possible), the Court will address now Defendant's argument that the Communication Decency Act (CDA) preempts Plaintiff's claim. Defendant argues that its conduct was an effort to identify and remove child-exploitation and objectionable material from Twitter and as such falls within the preemptive scope of Section 230(c)(2)(A) of the CDA. Plaintiff contends that nothing in the Complaint alleged that Defendant's actions fall under the scope of the CDA and that since it is an affirmative defense, the Court should not grant the motion unless the Complaint pleads every element of the defense.

The CDA Section 230(c)(2) provides:

No provider or user of an interactive computer service shall be held liable on account of—

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected;

47 U.S.C. § 230(c)(2). Section 230 preempts causes of action and liability that "may be imposed under any State or local law that is inconsistent with this section." *Id.* § 230(e)(3).

---

[3] *See, e.g.*, *Monroy v. Shutterfly, Inc.*, No. 16 C 10984, 2017 WL 4099846, at *3–5 (N.D. Ill. Sept. 15, 2017) (rejecting Shutterfly's arguments that a scan of face geometry cannot be done on photographs); *Vance v. Microsoft Corp.*, 525 F. Supp. 3d 1287, 1296 (W.D. Wash. 2021) (finding that facial scans taken from photographs are biometric identifiers because they are "a set of measurements of a specified physical component ... used to identify a person."). Further, as the Defendant notes, it is undisputed that a facial geometry scan can be derived from a photograph and considered a biometric identifier under BIPA. *See* Doc. [19] at 4.

[4] S*ee, e.g.*, *Sosa*, 600 F. Supp. 3d at 873 ("items identified as 'biometric identifiers' are 'specific, biology-based measurements used to identify a person, without reference to how the measurements were taken[.]'"); *Vance*, 525 F. Supp. 3d at 1296 ("The bottom line is that a 'biometric identifier' is . . . a set of measurements of a specified physical component ... used to identify a person.").

At the outset, Defendant cited no case law where a court held the CDA preempted a BIPA claim and the Court found none. Defendant further asserts that it is entitled to immunity under § 230(c)(2)(A) because it is a provider of an interactive computer service that acted voluntarily in good faith to restrict access to explicit images. Immunity under § 230(c)(2) is an affirmative defense so the Defendant bears the burden of proof. As CDA immunity frequently turns on facts not before the court at the pleading stage, dismissal is only appropriate when a plaintiff pleads themselves out of court. *Bonilla v. Ancestry.com Operations Inc.*, 574 F. Supp. 3d 582, 592 (N.D. Ill. 2021); *see Hyson USA, Inc. v. Hyson 2U, Ltd.*, 821 F.3d 935, 939 (7th Cir. 2016). Here, Plaintiff has not pled himself out of court. Taking the allegations in the light most favorable to Plaintiff, the Complaint does not allege that X acted in good faith, as required for immunity under § 230(c)(2). As such, Defendant is not entitled to immunity at this time.

Conclusion

For the reasons stated above, Defendant's motion to dismiss [15] is granted. Plaintiff may refile an amended complaint if he can cure the deficiencies and such an amendment is consistent with his obligations under Federal Rule of Civil Procedure 11. *Runnion ex rel. Runnion v. Girl Scouts of Greater Chicago & Nw. Indiana*, 786 F.3d 510, 519–20 (7th Cir. 2015) ("Unless it is certain from the face of the complaint that any amendment would be futile or otherwise unwarranted, the district court should grant leave to amend after granting a motion to dismiss."). If Plaintiff does not file an amended complaint by June 27, 2024, then the dismissal will automatically convert to a dismissal with prejudice.

SO ORDERED.

Dated: June 13, 2024
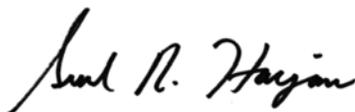
_____
Sunil R. Harjani
United States District Judge

7