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

In re Clearview AI, Inc., Consumer Privacy Litigation,	)	Case No. 21-cv-0135
	)	Judge Sharon Johnson Coleman

MEMORANDUM OPINION AND ORDER

Plaintiffs brought a first amended consolidated class action complaint in this multi-district litigation against the "Clearview defendants," which include Clearview AI, Inc., Hoan Ton-That, Richard Schwartz, Thomas Mulcaire, and Rocky Mountain Data Analytics LLC. Plaintiffs bring claims under the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* ("BIPA"), as well as statutory and common law claims under Virginia, California, and New York law. Before the Court is the Clearview defendants' motion to dismiss under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). For the following reasons, the Court grants in part and denies in part the Clearview defendants' motion.

Background

The Court presumes familiarity with its prior rulings in this multi-district litigation. In their first amended consolidated class action complaint, plaintiffs allege that the Clearview defendants' conduct violated their privacy rights and that defendants' use of their biometric information was without their knowledge and consent. Plaintiffs specifically allege that the Clearview defendants covertly scraped over three billion photographs of facial images from the internet and then used artificial intelligence algorithms to scan the face geometry of each individual depicted to harvest the individuals' unique biometric identifiers and corresponding biometric information.

The centerpiece of this multi-district litigation and plaintiffs' class action lawsuit is BIPA. The Illinois General Assembly "enacted BIPA in 2008 in response to the growing use of biometrics

'in the business and security screening sectors.'" *Fox v. Dakkota Integrated Sys., LLC,* 980 F.3d 1146, 1149 (7th Cir. 2020) (quoting 740 ILCS 14/5). The legislative findings include:

> Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, 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 Illinois General Assembly further concluded that "[t]he 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).

The Illinois Supreme Court has explained that through BIPA, "our General Assembly has codified that individuals possess a right to privacy in and control over their biometric identifiers and biometric information." *Rosenbach v. Six Flags Entm't Corp.,* 129 N.E.3d 1197, 1206, 432 Ill.Dec. 654, 663, 2019 IL 123186, ¶ 33 (Ill. 2019). As the Seventh Circuit has noted, BIPA "is designed to protect consumers against the threat of irreparable privacy harms, identity theft, and other economic injuries arising from the increasing use of biometric identifiers and information by private entities." *Bryant v. Compass Group USA, Inc.*, 958 F.3d 617, 619 (7th Cir. 2020).

Legal Standards

A Rule 12(b)(1) motion challenges federal jurisdiction, including Article III standing, and the party invoking jurisdiction bears the burden of establishing the elements necessary for subject matter jurisdiction, including standing. *Thornley v. Clearview AI, Inc.*, 984 F.3d 1241, 1244 (7th Cir. 2021); *International Union of Operating Eng'rs v. Daley*, 983 F.3d 287, 294 (7th Cir. 2020). Under Rule 12(b)(1), the Court accepts all well-pleaded factual allegations as true and construes all reasonable inferences in the plaintiff's favor when a defendant is facially attacked standing. *Prairie Rivers Network v. Dynegy Midwest Generation, LLC*, 2 F.4th 1002, 1007 (7th Cir. 2021).

A motion to dismiss pursuant to Rule 12(b)(6) for failure to state a claim tests the sufficiency

of the complaint, not its merits. *Skinner v. Switzer*, 562 U.S. 521, 529, 131 S.Ct. 1289, 179 L.Ed.2d 233 (2011). When considering dismissal of a complaint, the Court accepts all well-pleaded factual allegations as true and draws all reasonable inferences in favor of the plaintiff. *Erickson v. Pardus*, 551 U.S. 89, 94, 127 S.Ct. 2197, 167 L.Ed.2d 1081 (2007) (per curiam). To survive a motion to dismiss, plaintiff must "state a claim for relief that is plausible on its face." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007). A complaint is facially plausible when the plaintiff alleges enough "factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009).

Discussion

First Amendment

The Court starts with the parties' First Amendment arguments, keeping in mind that state statutes are presumed constitutional. *Heller v. Doe by Doe*, 509 U.S. 312, 320, 113 S.Ct. 2637, 125 L.Ed.2d 257 (1993). The Supreme Court recognizes that First Amendment protections and state-protected privacy interests can clash. *See The Florida Star v. B.J.F.,* 491 U.S. 524, 533, 109 S.Ct. 2603, 105 L.Ed.2d 443 (1989). As the *Florida Star* Court reasoned, "the sensitivity and significance of the interests presented in clashes between First Amendment and privacy rights counsel relying on limited principles that sweep no more broadly than the appropriate context of the instant case." *Id.* at 533. Accordingly, at this stage of the proceedings, the Court must review plaintiffs' allegations in detail and examine the First Amendment arguments narrowly in order to strike a balance between privacy interests and the interests protected by the First Amendment. *See id.*; *Snyder v. Phelps*, 562 U.S. 443, 462, 131 S.Ct. 1207, 179 L.Ed.2d 172 (2011) (Breyer, J., concurrence).

Viewing plaintiffs' allegations as true and in their favor, plaintiffs allege the Clearview defendants covertly scraped over three billion photographs of facial images from the internet and

then used artificial intelligence algorithms to scan the face geometry of each photograph to harvest the individuals' unique biometric identifiers and information. Clearview then created a searchable database containing this biometric information and data that allows users to identify unknown individuals by uploading a photograph to the database. The database can be searched remotely by licensed users of Clearview's web application. Plaintiffs further allege that the Clearview defendants have collected, captured, or otherwise obtained their biometric data without notice and consent, and thereafter, sold or otherwise profited from their biometric information.

Here, the Clearview defendants maintain that the capture of faceprints from public images and Clearview's analysis of the public faceprints is protected speech, and thus, BIPA violates the First Amendment by inhibiting Clearview's ability to collect and analyze public information. *See Sorrell v. IMS Health Inc.,* 564 U.S. 552, 570, 131 S.Ct. 2653, 180 L.Ed.2d 544 (2011) ("This Court has held that the creation and dissemination of information are speech within the meaning of the First Amendment."). Plaintiffs, however, assert that the capturing of faceprints and the action of extracting private biometric identifiers from the faceprints is unprotected conduct. *See Rumsfeld v. Forum for Acad. & Institutional Rights, Inc.*, 547 U.S. 47, 66, 126 S. Ct. 1297, 164 L.Ed. 2d 156 (2006).

The Clearview defendants' argument oversimplifies plaintiffs' allegations. Although Clearview captures public photographs from the internet, according to plaintiffs' allegations, Clearview then harvests an individual's unique biometric identifiers and information—which are not public information— without the individual's consent. Put differently, plaintiffs assert that the Clearview defendants' business model is not based on the collection of public photographs from the internet, some source code, and republishing information via a search engine, but the additional conduct of harvesting nonpublic, personal biometric data. And, as plaintiffs further allege, unlike fingerprints, facial biometrics are readily observable and present a grave and immediate danger to

privacy, individual autonomy, and liberty. *See Fox*, 980 F.3d at 1155 (biometric identifiers "are immutable, and once compromised, are compromised forever").

Accordingly, Clearview's process in creating its database involves both speech and nonspeech elements. When these "elements are combined in the same course of conduct, a sufficiently important governmental interest in regulating the nonspeech element can justify incidental limitations on First Amendment freedoms." *United States v. O'Brien*, 391 U.S. 367, 376, 88 S.Ct. 1673, 20 L.Ed.2d 672 (1968). Under these circumstances, the Court applies the intermediate scrutiny standard elucidated in *O'Brien*, namely, a regulation does not violate the First Amendment if (1) it is within the power of the government to enact, (2) furthers an important government interest, (3) the governmental interest is unrelated to the suppression of free expression, and (4) any incidental restriction on speech is no greater than is necessary to further the government interest. *Id.* at 377; *Foxxxy Ladyz Adult World, Inc. v. Village of Dix, Ill.*, 779 F.3d 706, 712 (7th Cir. 2015).

The parties do not discuss the power of the Illinois General Assembly to enact BIPA, therefore, the Court turns to the second *O'Brien* prong. The General Assembly enacted BIPA to protect Illinois residents' highly sensitive biometric information from unauthorized collection and disclosure. *See* 740 ILCS 14/5(c); *Rosenbach,* 129 N.E.3d at 1206. Next, BIPA, including its exceptions, does not restrict a particular viewpoint nor target public discussion of an entire topic under the third *O'Brien* requirement. *See Reed v. Town of Gilbert, Ariz.*, 576 U.S. 155, 169, 135 S.Ct. 2218, 192 L.Ed.2d 236 (2015); *Dahlstrom v. Sun-Times Media, LLC*, 777 F.3d 937, 944 n.5 (7th Cir. 2015). Under *O'Brien's* fourth factor, BIPA is narrowly tailored by legitimately protecting Illinois residents' highly sensitive biometric information and data, yet allowing residents to share their biometric information through its consent provision. *See, e.g., People v. Austin*, 155 N.E.3d 439, 468, 440 Ill.Dec. 669, 698, 2019 IL 123910, ¶ 93 (Ill. 2019) (discussing Illinois' revenge porn statute). Last, BIPA is not overly-broad. *See Center for Individual Freedom v. Madigan*, 697 F.3d 464, 471 (7th

Cir. 2012) ("A statute is facially overbroad only when 'it prohibits a substantial amount of protected speech.'") (quoting *United States v. Williams,* 553 U.S. 285, 292, 128 S.Ct. 1830, 170 L.Ed.2d 650 (2008)). The Court denies defendants' motion to dismiss in this respect.

Extraterritoriality Doctrine

The Court next turns to the Clearview defendants' contention that plaintiffs' BIPA claims violate Illinois' extraterritoriality doctrine. Because BIPA does not expressly intend to operate extraterritorially, the alleged BIPA violations must have taken place in Illinois. *See Avery v. State Farm Mut. Auto. Ins. Co.*, 216 Ill.2d 100, 296 Ill.Dec. 448, 835 N.E.2d 801, 852 (Ill. 2005). In *Avery*, the Illinois Supreme Court concluded that "there is no single formula or bright-line test for determining whether a transaction occurs within this state." *Id.* at 187. The critical question is whether the circumstances relating to the violations occurred "primarily" and "substantially" in Illinois. *Id.* In making this inquiry, courts look to "the residency of the plaintiff, the location of harm, communications between parties (where sent and where received), and where a company policy is carried out." *Rivera v. Google Inc.*, 238 F.Supp.3d 1088, 1101 (N.D. Ill. 2017) (Chang, J.).

Plaintiffs allege that the Illinois subclass are Illinois residents, the Clearview defendants failed to provide notice to the Illinois subclass members in Illinois, and defendants trespassed on the Illinois subclass members' private domains in Illinois. Also, plaintiffs maintain that defendants have contracted with hundreds of Illinois entities, both public and private. Construing the allegations in plaintiffs' favor, they have plausibly alleged that the relevant BIPA violations occurred primarily and substantially in Illinois despite Clearview's contention that the alleged violations took place in New York because the scraping of facial images and creation of the searchable database took place there. That said, the Court, recognizes that the application of the extraterritoriality doctrine is a fact intense inquiry that is best left for summary judgment once the parties have completed discovery. *See Rivera*, 238 F.Supp.3d at 1102; *Vance v. IBM*, Case No. 20 C 0577, 2020 WL 5530134, at *3 (N.D. Ill. Sept.

2020) (Kocoras, J.). The Court denies defendants' motion to dismiss based on the extraterritoriality doctrine.

Dormant Commerce Clause

The Clearview defendants also argue that BIPA, as sought to be applied here, violates the Dormant Commerce Clause of the United States Constitution. "While the Commerce Clause, U.S. CONST. art. I § 8, cl. 3, explicitly grants Congress the authority to regulate commerce among the States, it has long been understood that it also directly limits the power of the States to discriminate against or burden interstate commerce." *Alliant Energy Corp. v. Bie*, 330 F.3d 904, 911 (7th Cir. 2003). The restraint on the power of states to regulate commerce is referred to as the Dormant Commerce Clause. *Regan v. City of Hammond, Ind.*, 934 F.3d 700, 702 (7th Cir. 2019). The Dormant Commerce Clause prohibits "the application of a state statute to commerce that takes places wholly outside of the State's borders, whether or not the commerce has effects within the State." *Healy v. Beer Inst., Inc.*, 491 U.S. 324, 336, 109 S.Ct. 2491, 105 L.Ed.2d 275 (1989).

As discussed, plaintiffs have plausibly alleged that the BIPA violations occurred primarily and substantially in Illinois, therefore, the violations did not take place "wholly outside" of Illinois. Meanwhile, in support of their argument, the Clearview defendants rely on facts that are not alleged in the first amended consolidated class action complaint, including that Illinois residences make up only a small percentage of its database—facts the Court cannot consider at this juncture. *See Smith v. Burge*, 222 F.Supp.3d 669, 691 (N.D. Ill. 2016) (St. Eve, J.) ("defendant cannot, in presenting its 12(b)(6) challenge, attempt to refute the complaint or to present a different set of allegations") (citation omitted). As with the Clearview defendants' related extraterritoriality arguments, whether BIPA controls commercial conduct that occurs wholly outside Illinois is a question best left for later in these proceedings after the parties have completed discovery. *See Rivera*, 238 F.3d at 1104; *Vance*,

2020 WL 5530134, at *3. The Court denies defendants' motion to dismiss based on the Dormant Commerce Clause.

BIPA and Photographs

The Clearview defendants additionally argue that under the plain language of the statute, BIPA expressly excludes photographs and information derived from photographs from its reach. To explain, BIPA defines biometric identifier as follows:

> "Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color[.]

740 ILCS 14/10.

In support of their argument, the Clearview defendants do not mention the Northern District of Illinois cases that have addressed this exact argument, nor do they mention this argument in their reply brief. This is probably because Illinois courts have uniformly rejected the argument that BIPA exempts biometric data extracted from photographs. As Judge Chang explained in *Rivera*, a "'biometric identifier' is not the underlying medium itself, or a way of taking measurements, but instead is a set of measurements of a specified physical component (eye, finger, voice, hand, face) used to identify a person." *Rivera*, 238 F.Supp.3d at 1096; *see also Flores v. Motorola Solutions, Inc.*, No. 21-cv-1128, 2021 WL 232627, at *3 (N.D. Ill. Jan. 8, 2021) (Norgle, J.) ("The Court cannot say that those protections do not apply to any publicly published photographs of individuals—especially given that the biometric data in this case is the facial geometry of the class members, in contrast to the photos themselves."). The Court finds these opinions persuasive and denies defendants' motion to dismiss on this basis.

Individual Defendants' Liability

Next, defendants assert that the individual defendants, Ton-That, and Schwartz, should be

dismissed from this lawsuit because they cannot be held liable for actions they took as Clearview's officers or employees. In response, plaintiffs argue that the individual defendants can be liable for Clearview's conduct because they personally participated in the alleged tortious conduct, and, in the alternative, are alter egos of Clearview. Defendants note that the law of the state of incorporation, Delaware, applies to plaintiffs' arguments. *On Command Video Corp. v. Roti*, 705 F.3d 267, 272 (7th Cir. 2013) ("veil-piercing claims are governed by the law of the state of the corporation whose veil is sought to be pierced"). Plaintiffs maintain that Illinois and Delaware law yield the same result.

Examining the personal participation doctrine, "[a]s the human through which the corporate principal acts, '[a] corporate officer can be held personally liable for the torts he commits and cannot shield himself behind a corporation when he is a participant.'" *Prairie Capital III, L.P. v. Double E Holding Corp.*, 132 A.3d 35, 60 (Del. Ch. 2015) (citation omitted); *see also Brasby v. Morris*, Case No. 05C-10-022-RFS, 2007 WL 949485, at *8 (Del. Super. Mar. 9, 2007) ("The personal participation doctrine stands for the idea that, in certain situations, an officer in a corporation can be held liable for his own wrongful acts."). Likewise, under Illinois law, "[c]orporate officers are generally not liable for corporate obligations," however, they "are liable for any tort of the corporation in which they participate." *IOS Capital, Inc. v. Phoenix Printing, Inc.,* 808 N.E.2d 606, 611, 283 Ill.Dec. 640, 348 Ill.App.3d 366 (4th Dist. 2004).

Plaintiffs allege that Ton-That, the co-founder and Chief Executive Officer of Clearview, and Schwartz, the co-founder and Clearview's President, participated in, consented to, approved, authorized, and directed the wrongful acts alleged in the complaint.[1] Further, plaintiffs state that Ton-That and Schwartz authorized and directed the scheme to collect and distribute biometrics, executed agreements on Clearview's behalf, and treated the biometric database as their own.

[1] Plaintiffs do not argue that Clearview's General Counsel, Thomas Mulcaire, personally participated in the privacy torts by directing, ordering, ratifying, approving, or consenting to the tortious acts. Therefore, he is not individually liable for Clearview's actions.

Plaintiffs' allegations—viewed in their favor—plausibly suggest that Ton-That and Schwartz acted outside of their corporate capacities because these corporate officers personally participated in the privacy tort by directing, ordering, ratifying, approving, or consenting to the tortious act. *See Brandt v. Rokeby Realty Co.*, Case No. C.A. 97C-10-132-RFS, 2004 WL 2050519, at *10 (Del. Super. Sept. 8, 2004). Because plaintiffs have adequately alleged that Ton-That and Schwartz acted outside of their corporate capacities when they personally violated BIPA and plaintiffs' other privacy claims, the Court denies defendants' motion to dismiss individual defendants Ton-That and Schwartz. These allegations also defeat defendants' fiduciary shield arguments, *see Mutnick v. Clearview AI, Inc.*, Nos. 20 C 0512, 20 C 0846, 2020 WL 4676667, at *3 (N.D. Ill. Aug. 12, 2020) (Coleman, J.), arguments that defendants developed for the first time in their reply brief. *See White*, 8 F.4th at 552 ("arguments raised for the first time in [a] reply brief are waived").

As to the parties' alter ego/veil piercing arguments, "Delaware courts consider a number of factors in determining whether to disregard the corporate form and pierce the corporate veil, including: '(1) whether the company was adequately capitalized for the undertaking; (2) whether the company was solvent; (3) whether corporate formalities were observed; (4) whether the dominant shareholder siphoned company funds; and (5) whether, in general, the company simply functioned as a façade for the dominant shareholder.'" *Manichaean Capital, LLC v. Exela Tech., Inc.*, 251 A.3d 694, 706 (Del. Ch. 2021) (citation omitted); *see also Steiner Elec. Co. v. Maniscalco*, 51 N.E.3d 45, 57, 401 Ill.Dec. 852, 864, 2016 IL App (1st) 132023, ¶ 47 (1st Dist. 2016). In addition, both Illinois and Delaware law "require[] that the corporate structure cause fraud or similar injustice." *Wallace ex rel. Cencom Cable Income Partners II, Inc., L.P. v. Wood*, 752 A.2d 1175, 1184 (Del. Ch. 1999); *Gajda v. Steel Solutions Firm, Inc.*, 39 N.E.3d 263, 272, 395 Ill.Dec. 796, 805, 2015 IL App (1st) 142219, ¶ 23 (1st Dist. 2015).

Although there are some allegations in plaintiffs' first amended complaint that corporate formalities were not always observed at Clearview, such as Clearview directing its customers to send payments to Schwartz's personal residence and that Schwartz paid for the servers and other costs necessary to carry out Clearview's scraping and biometric scanning operations, plaintiffs have not adequately alleged any other veil piercing factors. For instance, viewing the allegations in their favor, plaintiffs have not provided sufficient factual detail that Clearview simply functioned as Ton-That's and Schwartz's façade. Furthermore, plaintiffs' complaint lacks detailed allegations supporting their argument that Ton-That and Schwartz undercapitalized Clearview. In the end, plaintiffs' allegations supporting their alter ego theory of individual liability as to Ton-That and Schwartz do not withstand defendants' motion to dismiss, especially because piercing the corporate veil is disfavored under both Delaware and Illinois law. *Judson Atkinson Candies, Inc. v. Latini–Hohberger Dhimantec,* 529 F.3d 371, 379 (7th Cir. 2008); *see also Wallace ex rel. Cencom Cable Income Partners II, Inc., L.P. v. Wood*, 752 A.2d 1175, 1183 (Del. Ch. 1999) ("Persuading a Delaware court to disregard the corporate entity is a difficult task.") (citation omitted). The Court grants defendants' motion in relation to these alter ego allegations.

Defendant Rocky Mountain[2]

Plaintiffs seek to pierce Rocky Mountain Data Analytics' LLC corporate veil to hold the parent company, Clearview, liable for Rocky Mountain's actions. By way of background, Thomas Mulcaire was Clearview's General Counsel and Vice President of defendant Rocky Mountain during the relevant time period, and Rocky Mountain was a special purpose entity used for the sole purpose

[2] In a cursory footnote in their opening brief, defendants argue Thomas Mulcaire and Rocky Mountain should also be dismissed because the Court lacks personal jurisdiction over them. Defendants have waived this argument. *See White v. United States*, 8 F.4th 547, 552 (7th Cir. 2021) ("perfunctory and undeveloped arguments, as well as arguments that are unsupported by pertinent authority, are waived."). Moreover, defendants' February 2, 2022 notice of supplemental authority adds little, if anything, to their waived argument.

of contracting with the Illinois Secretary of State. Rocky Mountain provided the Illinois Secretary of State access to the Clearview database and biometrics contained therein.

In Delaware, parent "liability may be permissible under either of two distinct theories: (1) the alter ego theory, or (2) the agency theory." *British Telecomm. v. IAC/InteractiveCorp*, 356 F.Supp.3d 405, 409 (D. Del. 2019). Under the agency theory, "a parent corporation is held liable for the actions of its subsidiary if the parent directed or authorized those actions." *Id.* (citation omitted); *see also Chrysler Corp. (Delaware) v. Chaplake Holdings, Ltd.*, 822 A.2d 1024, 1035 (Del. 2003). "Stated another way, when a subsidiary acts as the agent of the parent corporation, the parent corporation may be liable for actions conducted by the agent." *British Telecomm.*, 356 F.Supp.3d at 409. For "a parent corporation to be liable under the agency test, there must be a 'close connection between the relationship of the corporations and the cause of action,' focusing on 'the arrangement between the parent and the subsidiary, the authority given in that arrangement, and the relevance of that arrangement to the plaintiff's claim.'" *Garza v. Citigroup Inc.,* 192 F.Supp.3d 508, 514 (D. Del. 2016) (citation omitted).

Plaintiffs have plausibly alleged that Rocky Mountain acted as an agent of Clearview. Specifically, they assert Ton-That and Schwartz were directly involved in the creation of Rocky Mountain and were responsible for allowing Rocky Mountain to sell access to the Clearview database to its sole customer, the Illinois Secretary of State. Plaintiffs further allege that Ton-That, Schwartz, and Mulcaire authorized and directed a Clearview salesperson to double as a Rocky Mountain salesperson, knowing that the salesperson would be paid by Clearview. Plaintiffs also state that Ton-That and Schwartz authorized Mulcaire to provide his personal information to the Illinois Secretary of State, resulting in the Illinois Secretary of State submitting a voucher to the Illinois Comptroller authorizing payment to Mulcaire. Other allegations include that Rocky Mountain's activities, which included collecting, obtaining, distributing, disseminating, selling,

leasing, and profiting from the biometrics, were at the direction of Ton-That and Schwartz. Not only did Ton-That and Schwartz fail to adequately capitalize Rocky Mountain, they admit that Rocky Mountain had no actual operations. Last, defendants have waived their argument made for the first time in their reply brief that Mulcaire and Rocky Mountain are exempt based on 740 ILCS 14/25(e). *See White*, 8 F.4th at 552. The Court therefore denies this aspect of defendants' motion.

BIPA Section 15(c) Claim

Defendants next contend that plaintiffs have failed to sufficiently allege a claim under 740 ILCS 14/15(c), which prohibits private entities from selling, leasing, trading, or otherwise profiting from a person's biometric identifiers or information. Defendants specifically argue that none of plaintiffs' factual allegations describes Clearview's customers receiving access to the Clearview database or that the customers received access to plaintiffs' biometric information. Despite this argument, the first amended consolidated class action complaint repeatedly states (1) defendants developed their technology for their own profit; (2) defendants sold, distributed, disseminated, traded, leased, and otherwise profited from the biometric database; (3) defendants sold access to the database to more than 200 private companies who searched the biometric database for their business purposes; and (4) defendants profited from selling access to the database. Plaintiffs' allegations state a plausible BIPA 15(c) claim. *See Iqbal*, 556 U.S. at 679 ("Determining whether a complaint states a plausible claim for relief" is "a context-specific task that requires the reviewing court to draw on its judicial experience and common sense.").

Nevertheless, defendants maintain that the statute's language "otherwise profit from" indicates that BIPA 15(c) prohibits only the sale of biometric data, not the business of using biometric technology. At its core, plaintiffs' claim concerns the sale of biometric data because the Clearview defendants' business model is premised on collecting and capturing biometric data and then profiting from that data when customers pay to search the Clearview database. Thus, when a

customer pays to search the database containing plaintiffs' biometric information to find a potential match, defendants profit from plaintiffs' biometric data in violation of BIPA 15(c). *See Flores,* 2021 WL 232627, at *3. Therefore, defendants' argument is without merit.

Standing for State Law Claims

The Clearview defendants additionally argue that plaintiffs do not have Article III standing to bring their claims under California, Virginia, and New York state law. "Article III of the Constitution limits the federal judicial power to deciding 'Cases' and 'Controversies'" and "as an essential part of a federal court's authority under Article III, [the] standing doctrine ensures respect for these jurisdictional bounds." *Prairie Rivers Network,* 2 F.4th at 1007. To establish standing under Article III, a plaintiff must show: (1) he suffered an injury-in-fact; (2) that is fairly traceable to the defendants' conduct; and (3) that is likely to be redressed by a favorable judicial decision. *Cothron v. White Castle System, Inc.,* 20 F.4th 1156, 1160 (7th Cir. 2021). Under the first requirement, an injury-in-fact must be "concrete and particularized" and "actual or imminent." *Prosser v. Becerra*, 2 F.4th 708, 713 (7th Cir. 2021). Defendants focus on the injury-in-fact requirement arguing that plaintiffs have not suffered any cognizable injuries, such as identity theft.

To determine whether the disclosure of plaintiffs' private information caused a sufficiently concrete harm to support standing, courts look to both history and the judgment of Congress for guidance. *Gadelhak v. AT&T Servs., Inc.*, 950 F.3d 458, 462 (7th Cir. 2020) (Barrett, J.). The historical inquiry asks, "whether the asserted harm has a 'close relationship' to a harm traditionally recognized as providing a basis for a lawsuit in American courts—such as physical harm, monetary harm, or various intangible harms." *TransUnion, LLC v. Ramirez*, 141 S.Ct. 2190, 2200 (2021). As the *TransUnion* Court clarified, "[v]arious intangible harms can also be concrete" including "reputational harms, disclosure of private information, and intrusion upon seclusion." *Id.* at 2204.

Plaintiffs have sufficiently alleged that defendants' disclosure of their private information without their consent caused them the concrete harm of violating their privacy interests in their biometric data. In addition, the nonconsensual taking of plaintiffs' private information is a concrete harm because the possibility of misuse is ever present. Because plaintiffs have sufficiently alleged a concrete harm supporting Article III standing, the Court denies defendants' motion in this respect.

Virginia State Law Claims

In Counts Eight and Nine of the first amended consolidated class action complaint, plaintiff Shelby Zelonis Roberson, on behalf of herself and others similarly situated in the Virginia Subclass, brings two claims under Virginia law, including, the Virginia statute prohibiting the unauthorized use of names or pictures, Virginia Code § 8.01-40(A), as alleged in Count Eight. Virginia Code § 8.01-40(A) states:

> Any person whose name, portrait, or picture is used without having first obtained the written consent of such person, or if dead, of the surviving consort and if none, of the next of kin, or if a minor, the written consent of his or her parent or guardian, ***for advertising purposes or for the purposes of trade***, such persons may maintain a suit in equity against the person, firm, or corporation so using such person's name.

(emphasis added).

In their motion, defendants argue plaintiffs have failed to allege that defendants used their likenesses for advertising purposes, but the statute unequivocally states that plaintiffs may also establish a claim under § 8.01-40(A) if defendants used their likenesses for the purposes of trade. *Town & Country Prop. Inc. v. Riggins*, 457 S.E.2d 356, 362, 249 Va. 387, 394 (Va. 1995) ("Use for 'advertising purposes' and use 'for the purposes of trade' are separate and distinct statutory concepts."). "In determining whether the use was 'for the purposes of trade,' courts are to consider whether the [picture] was used to draw trade to an entity." *Goodweather v. Parekh*, No. 20-cv-0006, 2020 WL 9259760, at *10 (E.D. Va. Sept. 18, 2020). Here, plaintiffs have sufficiently alleged that

the Clearview defendants profited from the unconsented use of their likenesses under "for purposes of trade."

Nonetheless, the Clearview defendants maintain plaintiffs' publicity right claim fails because the use of plaintiffs' photographs or likeness has a protected public interest purpose. *See Wiest v. E-Fense, Inc.*, 356 F.Supp.2d 604, 611 (E.D. Va. 2005) ("If a name or likeness is used without consent in connection with matters that are 'newsworthy' or of 'public interest,' the statute does not apply."). In particular, defendants argue that the right to publicity must yield to constitutional free speech interests. Keeping in mind that a motion to dismiss concerns the sufficiency of the allegations, the Court rejects defendants' argument because, as plaintiffs have alleged, the Clearview defendants scraped plaintiffs' photographs to build a database from which defendants profited and that this conduct did not have any connection to public affairs. Defendants' cursory arguments about "speech interests" does not change this analysis. The Court denies defendants' motion to dismiss Count Eight.

In Count Nine, Roberson alleges the Clearview defendants violated Virginia's Computer Crimes Act ("VCCA"), Virginia Code § 18.2-152.1, *et seq*. *See Hately v. Watts*, 917 F.3d 770, 781 (4th Cir. 2019) ("The Virginia Computer Crimes Act is a criminal statute with a private civil right of action."). To establish a VCCA claim, plaintiffs must eventually prove the Clearview defendants: (1) used a computer or computer network; (2) without authority; and (3) either obtained property or services by false pretenses, embezzlement or larceny, or converted the property of another. *See Rosciszewski v. Arete Assoc., Inc.,* 1 F.3d 225, 230 (4th Cir. 1993); *Cvent, Inc. v. Eventbrite, Inc.,* 739 F.Supp.2d 927, 934 (E.D. Va. 2010).

Defendants first argue that plaintiffs have failed to allege an actual injury, but "[i]n Virginia, one holds a property interest in one's name and likeness." *Riggins*, 457 S.E.2d at 364. Here, plaintiffs have stated an actual injury based on their allegations that defendants converted their likenesses.

Defendants also contend plaintiffs have failed to sufficiently allege that Clearview used any computer or computer network without authority. Defendants' argument is without merit because plaintiffs allege that defendants scraped their images in violation of the terms of service of the websites on which their images were hosted and without the plaintiffs' consent and that defendants converted their property interest in their likenesses. In addition, defendants assert that plaintiffs failed "to allege false pretenses, conversion, artifice, tricker, or deception," although, as discussed, plaintiffs clearly allege that defendants converted their property interests. The Court denies defendants' motion to dismiss Count Nine.

California State Law Claims

In Counts Ten through Thirteen, plaintiff Andrea Vestrand, on behalf of herself and others similarly situated in the California Subclass, brings claims under California statutory and common law. In Count Ten, Vestrand alleges the Clearview defendants violated California's Unfair Competition Law ("UCL") by using her biometric information without her consent. To bring a claim under the UCL, a plaintiff must "(1) establish a loss or deprivation of money or property sufficient to quantify as injury in fact, i.e., *economic injury*, and (2) show that the economic injury was the result of, i.e., *caused by*, the unfair business practice." *Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 322, 120 Cal.Rptr.3d 741, 246 P.3d 877 (Cal. 2011) (emphasis in original).

Plaintiffs' UCL claim necessarily fails because personal information is not "property" for purposes of the UCL. *See In re Facebook Privacy Litig.*, 791 F.Supp.2d 705, 714 (N.D. Cal. 2011). Indeed, "[n]umerous courts have held that disclosure of personal information alone does not constitute economic or property loss sufficient to establish UCL standing, unless the plaintiff provides specific allegations regarding the value of the information." *Mastel v. Miniclip SA*, ___ F.Supp.3d ___, 2021 WL 2983198, at *11 (E.D. Cal. 2021).

Also, plaintiffs' UCL claim does not survive the Clearview defendants' motion to dismiss because plaintiffs have failed to plausibly allege an unfair business practice for purposes of the UCL. The UCL "governs 'anti-competitive business practices' as well as injuries to consumers, and has as a major purpose 'the preservation of fair business competition.'" *Chu v. Old Republic Home Protection Co., Inc.*, 274 Cal.Rptr.3d 528, 536, 60 Cal.App.5th 346, 357 (Cal. 2021). In sum, the "UCL's purpose is to protect both consumers and competitors by promoting fair competition in commercial markets for goods and services." *Erhart v. BofI Holding, Inc.,* 387 F.Supp.3d 1046, 1059 (S.D. Cal. 2019) (citation omitted). Plaintiffs' allegations do not involve the protection of fair competition in commercial markets for goods and services, and thus the Court dismisses plaintiffs' UCL claim without leave to amend because any such amendment would be futile. *See Always Towing & Recovery, Inc. v. City of Milwaukee*, 2 F.4th 695, 707 (7th Cir. 2021).

In Count Eleven, Vestrand alleges a commercial misappropriation of likeness claim against the Clearview defendants under California Civil Code § 3344(a), as well as a common law right to publicity claim in Count Twelve. The Court analyzes Counts Eleven and Twelve together because to state a claim under § 3344(a), a plaintiff must first fulfill the elements of the common law right to publicity. *See Downing v. Abercrombie & Fitch,* 265 F.3d 994, 1001 (9th Cir. 2001); *Cross v. Facebook, Inc.,* 222 Cal.Rptr.3d 250, 265, 14 Cal.App.5th 190, 208 (Cal. 2017) ("Civil Code section 3344 was intended to complement, not supplant, common law claims for right of publicity.").

The California common law "right of publicity seeks to prevent commercial exploitation of an individual's identity without that person's consent." *Maloney v. T3Media, Inc.*, 853 F.3d 1004, 1010 (9th Cir. 2017). The elements of a common law right to privacy claim include: (1) defendant's unauthorized use of the plaintiff's identity; (2) the appropriation of plaintiff's name or likeness to defendant's advantage, commercial or otherwise; and (3) the resulting injury. *Downing,* 265 F.3d at 1001; *Ross v. Roberts*, 166 Cal.Rptr.3d 359, 365, 222 Cal.App.4th 677, 684 (Cal. 2013).

The Clearview defendants argue that Vestrand's common law right to publicity claim fails because she does not have an economic interest in her likeness. Vestrand, however, is not required to plead facts corresponding to each legal element of her claim to survive a motion to dismiss, but instead, need only allege a plausible claim. *Chapman v. Yellow Cab Cooperative*, 875 F.3d 846, 848 (7th Cir. 2017). Vestrand has done so by alleging that the Clearview defendants used her photographs and likeness without authorization for commercial gain. Further, Vestrand alleges the California Subclass was injured because the Clearview defendants did not compensate them for the use of their likenesses, identifies, and photographs. These allegations plausibly state a common law right to publicity claim under California law.

Next, under California's statutory remedy, § 3344, plaintiffs must also show "a knowing use by the defendant as well as a direct connection between the alleged use and the commercial purpose." *Downing*, 265 F.3d at 1001. Defendants argue that § 3344 requires plaintiffs to allege that its use of the Clearview database was for purposes of advertising, selling, or soliciting. By making this argument, defendants ignore parts of § 3344(a), which states, "[a]ny person who knowingly uses another's name, voice, signature, photograph, or likeness ***in any manner***, on or in products, merchandise, or goods, or for purposes of advertising or selling, or soliciting purchases of, products, merchandise, goods or services, without such person's prior consent … shall be liable for any damages sustained by the person or persons injured as a result thereof." (emphasis added). Thus, under § 3344, plaintiffs need not allege that defendants used their photos or likenesses for purposes of advertising, selling, or soliciting as defendants argue As discussed, plaintiffs have adequately alleged the Clearview defendants knowingly used their photos by accessing the Clearview database for a profit. The Court denies defendants' motion to dismiss Counts Eleven and Twelve.

In Count Thirteen, Vestrand alleges defendants violated her right to privacy under the California Constitution. To establish a claim for invasion of privacy under the California

Constitution, a plaintiff must eventually show (1) she possesses a legally protected privacy interest, (2) she maintains a reasonable expectation of privacy, and (3) defendant's conduct constituted a serious invasion of privacy. *Hill v. National Collegiate Athletic Assn.*, 865 P.2d 633, 654-55, 26 Cal.Rptr.2d 834, 7 Cal.4th 1 (Cal. 1994).

Defendants argue Vestrand failed to plausibly allege that she possesses a legally protected privacy interest. The California Constitution protects two separate classes of privacy interests: (1) information privacy, which includes interests in precluding the dissemination or misuse of confidential and sensitive information; and (2) autonomy privacy, including interests in making personal decisions or conducting personal activities without intrusion. *In re Google Location History Litig.*, 514 F.Supp.3d 1147, 1154 (N.D. Cal. 2021). Because autonomy privacy protects bodily autonomy, it does not apply under the circumstances. *See In re Yahoo Mail Litig.*, 7 F.Supp.3d 1016, 1039 (N.D. Cal. 2014). The Court therefore examines whether plaintiffs have sufficiently alleged the first class of privacy interests, information privacy.

Vestrand has sufficiently alleged that the Clearview defendants' conduct constituted a serious invasion of her information privacy because biometric information, by its very nature, is sensitive and confidential. In addition, plaintiffs allege that the California Subclass had a reasonable expectation of privacy to their highly sensitive biometrics despite defendants' argument that they had no reasonable expectation of privacy over photographs they uploaded to public websites. Again, the Clearview defendants ignore that their conduct invades plaintiffs' privacy in their biometric information, not plaintiffs' mere photographs. Vestrand has therefore plausibly alleged her right to privacy claim under the California Constitution.

New York State Law Claim

In Count Fourteen, plaintiff Aaron Hurvitz, on behalf of himself and others similarly situated in the New York Subclass, brings a claim under New York's Civil Rights Act § 51. The

purpose of § 51 is to protect individuals from the commercial exploitation of their name or image. *See Kuklachev v. Gelfman*, 600 F.Supp.2d 437, 474-75 (E.D.N.Y. 2009). To establish liability under § 51, a plaintiff must show defendant's nonconsensual use of his name, portrait, picture, or voice within the state of New York for purposes of advertising or trade. *See Electra v. 59 Murray Enter.*, Inc., 987 F.3d 233, 249 (2d Cir. 2021).

The Clearview defendants argue Hurvitz has not sufficiently alleged that his picture was used for trade purposes. New York "courts have defined use 'for the purposes of trade' as use which 'would draw trade to the firm' or 'use for the purpose of making profit.'" *Amusement Indus., Inc. v. Stern*, 693 F.Supp.2d 301, 314 (S.D.N.Y. 2010) (citation omitted). Plaintiffs have repeatedly alleged the Clearview defendants developed technology to invade the privacy of the American public for their own profit. Accordingly, the Court denies defendants' motion to dismiss Count Fourteen.

Unjust Enrichment Claim

Next, the Clearview defendants move to dismiss plaintiffs' unjust enrichment claim alleged in Count Fifteen of the first amended consolidated class action complaint. In particular, defendants argue that unjust enrichment is not a viable, stand-alone claim under Illinois, Virginia, California, or New York law. Under Illinois law, unjust enrichment "is not a separate cause of action that, standing alone, would justify an action for recovery." *Toushin v. Ruggiero*, 2021 IL App (1st) 192171, ¶ 80, 2021 WL 2718495, at *13 (1st Dist. 2021)(quoting *Mulligan v. QVC, Inc.,* 888 N.E.2d 1190, 1200, 321 Ill.Dec. 257, 267, 382 Ill.App.3d 620, 631 (1st Dist. 2008). Rather, unjust enrichment is a condition resulting from unlawful or improper conduct like fraud and may be redressed by a cause of action based upon that improper conduct. *Toushin*, 2021 IL App (1st) 192171, ¶ 80. "[I]f an unjust enrichment claim rests on the same improper conduct alleged in another claim, then the unjust enrichment claim will be tied to this related claim—and, of course, unjust enrichment will stand or fall with the related claim." *Cleary v. Philip Morris Inc.*, 656 F.3d 511, 517 (7th Cir. 2011).

Because plaintiffs have sufficiently alleged their BIPA claims, the Court denies defendants' motion to dismiss the unjust enrichment claim attendant to the BIPA claims.

Under Virginia law, a claim of unjust enrichment requires a showing that the defendant received benefits of which the defendant was aware and that the defendant accepted or retained the benefit without paying for its value. *Fessler v. IBM Corp.,* 959 F.3d 146, 157 (4th Cir. 2020). Because plaintiffs have adequately that the Clearview defendants used the benefit of their biometric data without paying them for its value, the Court denies the Clearview defendants' motion to dismiss the Virginia unjust enrichment claim.

The Ninth Circuit has explained that a California common law unjust enrichment claim may survive either "as an independent cause of action or as a quasi-contract claim for restitution." *ESG Capital Partners, LP v. Stratos*, 828 F.3d 1023, 1038 (9th Cir. 2016); *see also Hart v. TWC Product & Tech. LLC*, 526 F.Supp.3d 592, 604 (N.D. Cal. 2021). "To allege unjust enrichment as an independent cause of action, a plaintiff must show that the defendant received and unjustly retained a benefit at the plaintiff's expense." *ESG Capital Partners,* 828 F.3d at 1028. Plaintiffs have sufficiently alleged defendants were unjustly enriched by the use of their biometric information without their consent.

The Clearview defendants, however, correctly assert plaintiffs' New York common law unjust enrichment claims are preempted by New York Civil Rights Act §§ 50, 51. *See Sondik v Kimmel,* 131 A.D. 3d 1041, 1042, 16 N.Y.S.3d 296, 298 (N.Y. App. Div. 2015) ("Common-law unjust enrichment claims for the unauthorized use of an image or likeness are preempted by Civil Rights Law §§ 50 and 51."); *Myskina v. Conde Nast Publications, Inc.,* 386 F.Supp.2d 409, 420 (S.D.N.Y. 2005) (same). The Court grants this aspect of defendants' motion to dismiss.

Declaratory Judgment Claim

On a final note, because defendants' argument for dismissing plaintiffs' declaratory and injunctive relief claim in Count Sixteen is solely based on plaintiffs' failure to state a claim, the Court denies defendants' motion to dismiss this count.

Conclusion

The Court grants in part and denies in part defendants' motion to dismiss [87].

IT IS SO ORDERED.

Date: 2/14/2022

Entered: 

SHARON JOHNSON COLEMAN
United States District Judge