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

| | |
|---|---|
| In re Clearview AI, Inc. Consumer Privacy Litigation | Civil Action File No.: 1:21-cv-00135<br>Judge Sharon Johnson Coleman<br>Magistrate Judge Maria Valdez |

**PLAINTIFFS' OPPOSITION TO CLEARVIEW DEFENDANTS' MOTION TO DISMISS**

## TABLE OF CONTENTS

INTRODUCTION ..... 1

FACTUAL BACKGROUND ..... 2

ARGUMENT ..... 4

I. Plaintiffs Plead Sufficient Facts to Hold the Individual Defendants Responsible for Clearview's Conduct ..... 4

II. The Complaint Alleges Facts Sufficient to Pierce Rocky Mountain's Corporate Veil ..... 6

III. Plaintiffs Have Sufficiently Pled Their Claims Against Rocky Mountain ..... 7

IV. Plaintiffs' BIPA Claims Do Not Violate the Extraterritoriality Doctrine ..... 7

V. The Dormant Commerce Clause Does Not Apply to Plaintiffs' BIPA Claims ..... 9

VI. The First Amendment Does Not Bar Plaintiffs' BIPA Claims ..... 11

A. BIPA Regulates Conduct – *i.e.*, the Collection and Use of Private Information ..... 11

B. There is No First Amendment Right to Access or Use Private Information ..... 13

C. The Regulated Conduct Is Not Sufficiently Expressive to Implicate the First Amendment ..... 15

D. Even If BIPA Burdens Speech, It Is Subject to Intermediate Scrutiny ..... 15

E. BIPA Withstands Intermediate Scrutiny ..... 18

VII. The Complaint Sufficiently Alleges a Violation of BIPA § 15(c) ..... 19

VIII. BIPA Applies to Biometrics Extracted from Photographs. ..... 20

IX. Plaintiffs Have Standing to Assert Their California, New York and Virginia Claims ..... 21

X. Plaintiffs' Sufficiently Plead Their Right of Publicity Claims ..... 23

XI. Count Nine States a Claim for Violations of the Virginia Computer Crimes Act ..... 26

XII. Count Ten Sufficiently Alleges a California Unfair Competition Claim.....28

XIII. Count Thirteen Sufficiently Alleges a California Constitutional Privacy Claim.....29

XIV. Plaintiff State Claims for Unjust Enrichment.....30

XV. Plaintiffs State a Claim for Declaratory Judgment or Injunctive Relief.....30

CONCLUSION.....30

## TABLE OF AUTHORITIES

## CASES

*Antman v. Uber Techs., Inc.,* 2015 WL 6123054 (N.D. Cal. Oct. 19, 2015)……21

*Avery v. State Farm Mut. Auto. Ins. Co.,* 835 N.E.2d 801 (Ill. 2005)……8

*Bartnicki v. Vopper,* 532 U.S. 514 (2001)…… .....18

*Brandt v. Rokeby Realty Co.,* 2004 WL 2050519 (Del. Super. Ct. Sept. 8, 2004) .....4

*Bryant v. Compass Group USA, Inc.*, 958 F.3d 617 (7th Cir. 2020).....8, 11, 22

*Callahan v. Ancestry.com Inc.*, 2021 WL 783524 (N.D. Cal. Mar. 1, 2021) .....24

*Clay v. Butler*, 112 S.E. 697 (Va. 1922) .....27

*Carpenter v. United States*, 138 S.Ct. 2206 (2018) .....12

*Dahlstrom v. Sun-Times Media*, LLC 777 F.3d 937 (7th Cir. 2015).....11, 13, 15, 17, 18

*Downing v. Abercrombie & Fitch*, 265 F.3d 994 (9th Cir. 2001).....24

*Fox v. Dakkota Integrated Sys., LLC*, 980 F.3d 1146 (7th Cir. 2020).....23, 29

*Flores v. Motorola Sols., Inc.,* 2021 WL 232627 (N.D. Ill. Jan. 8, 2021).....20

*Gadelhak v. AT&T Servs., Inc.*, 950 F.3d 458 (7th Cir. 2020) .....22

*Healy v. Beer Inst., Inc.,* 491 U.S. 324, 336 (1989).....9, 10

*Hilton v. Hallmark Cards*, 599 F.3d 894 (9th Cir. 2009) .....24

*hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985 (9th Cir. 2019) .....27

*In Re Facebook Biometric Info. Privacy Litig.*, 2018 WL 2197546
(N.D. Cal., May 14, 2018) .....9

*In re Facebook Biometric Privacy Litig.*, 185 F. Supp. 3d 1155
(N.D. Cal. 2016).....20

*In re Google, Inc. Priv. Pol'y Litig.*, 2012 WL 6738343 (N.D. Cal. Dec. 28, 2012).....21

*Junger v. Daley*, 209 F.3d 481 (6th Cir. 2000) .....15

*Kwikset Corp. v. Superior Ct.*, 51 Cal. 4th 310 (Cal. 2011) .....28

*Kyllo v. United States*, 533 U.S. 27 (2001) .....12, 29

*Law Ofcs. of Mathew Higbee v. Expungement Assistance Servs.*,
214 Cal. App. 4th 544 (Cal. Ct. App. 2013) .....28

*Landau v. CNA Fin. Corp.*, 886 N.E.2d 405 (Ill. App. Ct. 2008) .....9

*LeClercq v. Lockformer Co.*, 2002 WL 908037 (N.D. Ill. May 6, 2002) .....4

*Lerman v. Flynt Distrib. Co.*, 745 F.2d 123 (2d Cir. 1984) .....26

*Mainstream Mktg. Servs., Inc.* v. FTC, 358 F.3d 1228 (10th Cir. 2004) .....13

*Maloney v. T3Media, Inc.*, 853 F.3d 1004 (9th Cir. 2017) .....24

*Mason v. Network of Wilmington, Inc.*, 2005 WL 1653954 (Del. Ch. 2005) .....5

*Metrocall of Delaware v. Continental Cellular Corp.*, 437 S.E.2d 189 (Va. 1993) .....27

*Midwest Title Loans, Inc. v. Mills*, 593 F.3d 660 (7th Cir. 2010) ..... 10

*Miller v. Collectors Universe, Inc.*, 159 Cal. App. 4th 988 (Cal. Ct. App. 2008) ..... 23, 24

*Mobil Oil Corp. v. Linear Films, Inc.,* 718 F. Supp. 260 (D. Del. 1989) .....6

*Monroy v. Shutterfly*, Inc., 2017 WL 4099846 (N.D. Ill. Sept. 15, 2017) .....8, 9, 20, 21

*Moreno v. Hanford Sentinel, Inc.*, 172 Cal. App. 4th 1125 (Cal. Ct. App. 2009) .....29

*Morley-Murphy Co. v. Zenith Elecs. Corp.*, 142 F.3d 373 (7th Cir. 1998) .....9

*Morrison v. YTB Intern., Inc.*, 649 F.3d 533 (7th Cir. 2011) .....8

*Nat'l Coalition Of Prayer, Inc. v. Carter*, 455 F.3d 783 (7th Cir. 2006) .....13

*Offor v. Mercy Med. Ctr.*, 167 F. Supp. 3d 414 (E.D.N.Y. 2016) .....14

*Patel v. Facebook*, Inc., 932 F.3d 1264 (9th Cir. 2019) .....7, 12, 18

*People ex rel. Madigan v. Tang*, 346 Ill. App. 3d 277, 805 N.E.2d 243 (2004) .....5

*Phillips v. Bally Total Fitness Holding Corp.*, 865 N.E.2d 310 (Ill. App. Ct. 2007) .....9

*Reed v. Town of Gilbert*, 576 U.S. 155 (2015) .....15, 17

*Rivera v. Google*, Inc., 238 F.Supp.3d 1088 (N.D. Ill. 2017).....8, 9, 20, 21,

*RNS Servicing, LLC v. Spirit Constr. Servs., Inc.,* 2018 WL 3729326 (N.D. Ill. Aug. 6, 2018).....4

*Rosenbach v. Six Flags Entn't Corp.*, 129 N.E.3d 1197 (Ill. 2019) .....18

*Rumsfeld v. Forum for Academic. & Inst'l Rts., Inc.,* 547 U.S. 47 (2006) .....11, 15

*S. Dakota v. Wayfair, Inc*., 138 S. Ct. 2080 (2018) .....11

*Search King, Inc. v. Google Tech, Inc.*, 2003 WL 21464568 (W.D. Okla. May 27, 2003) .....15

*Sorrell v. IMS Health*, 564 U.S. 552 (2011) .....14, 16

*State of Ill. v. Austin,* 155 N.E.3d 439 (Ill. 2019) .....16, 18

*StrikeForce Techs., Inc. v. PhoneFactor, Inc.,* 2013 WL 6002850 (D. Del. Nov. 13, 2013), *as amended* (Nov. 14, 2013).....6

*Town & Country Props. v. Riggins*, 457 S.E.2d 356 (Va. 1995) .....25, 26, 27

*TransUnion, LLC v. Ramirez*, 549 U.S. ___ (2021), 2021 WL 2599472 (U.S. June 25, 2021) .....22

*Van Buren v. United States,* __ U.S. __, 141 S. Ct. 1648 (June 3, 2021).....27

*U.S. v. O'Brien*, 391 U.S. 367 (1968) .....11

*U.S. v. Miami University*, 294 F.3d 797 (6th Cir. 2002).....13

*Vance v. Int'l Business Machines Corp.* 2020 WL 5530134 (N.D. Ill. Sept. 15, 2020) .....7, 8, 9, 20

*Vulcan Golf, LLC v. Google Inc.,* 552 F.Supp.2d 752 (N.D. Ill. 2008).....9

*Wiest v. E-Fense, Inc.*, 356 F. Supp. 2d 604 (E.D. Va. 2005) .....23

*White v. Samsung Elecs. Am., Inc.*, 971 F.2d 1395 (9th Cir. 1992).....23

*Zinner v. Olenych*, 2015 WL 1372122 (E.D. Va. Dec. 24, 2015) .....23

## STATUTES

***Federal Statutes***

15 U.S.C. § 6501, *et seq*.....12

15 U.S.C. § 1681 ..... 12

20 U.S.C. § 1232g ..... 12

42 U.S.C. § 1320d, *et seq* ..... 12

***State Statutes***

Cal. Civ. Code § 1798.100 *et seq.* ..... 21

740 ILCS § 14/1, *et seq.* ..... 2

N.Y. State Tech. Law § 106-b ..... 21

Va. Code. Ann. § 8.01–40 ..... 23, 25, 27

Va. Code Ann. § 18.2-151.1 *et seq.* ..... 21, 26, 27, 28

Va. Code Ann. § 18.2-186.3 ..... 21, 26, 27, 28

**FEDERAL RULES AND REGULATIONS**

12 C.F.R. § 1016 ..... 17

**OTHER AUTHORITIES**

*American Heritage Dictionary*, www.ahdictionary.com ..... 25

Restatement (Second) of Torts § 652B (1977) ..... 23

Restatement (First) of Torts § 867 (1939) ..... 23

## INTRODUCTION

Defendants Clearview AI, Inc. ("Clearview"), Hoan Ton-That, Richard Schwartz, Thomas Mulcaire and Rocky Mountain Data Analytics LLC ("Rocky Mountain") (collectively "Defendants"; Ton-That, Schwartz and Mulcaire, collectively, the "Individual Defendants") have taken the proverbial kitchen-sink approach in seeking dismissal of Plaintiffs First Amended Consolidated Class Action Complaint (the "Complaint"). But none of Defendants' arguments changes the fact that Defendants scraped over three billion online images, unlawfully extracted Plaintiffs' and class members' sensitive biometric data from those images and then unlawfully used and distributed the images and sensitive data for their personal gain. Importantly, Defendants make no serious challenge to Plaintiffs' substantive claims, focusing most of their attention on procedural and legal issues. Where Defendants challenge the substantive claims, they improperly rely on information outside of the Complaint and otherwise fail to view Plaintiffs' allegations as true and in the light most favorable to Plaintiffs. Defendants' inability to challenge Plaintiffs' actual allegations is a tacit admission of the propriety of Plaintiffs' claims.

Defendants' procedural and legal challenges fare no better. As a threshold matter, the Individual Defendants can be held liable for Clearview's actions, and Clearview can be held liable for the Rocky Mountain's actions. Defendants reach a different result only by ignoring Plaintiffs' allegations and improperly framing the issues. Defendants' extraterritorial and dormant Commerce Clause challenges also fail, as they have been soundly rejected at the motion to dismiss stage by numerous courts. Defendants provide no basis for a different result here. While Defendants devote a lot of ink to their First Amendment challenge, they fail to acknowledge the simple fact that Illinois' Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, *et seq.*, regulates conduct – the collection and use of private information – not speech. To the extent BIPA has any impact

on speech, its regulations are content neutral and subject to intermediate scrutiny – which the statute easily withstands. Finally, Defendants' challenges to the standing of Plaintiffs Roberson, Vestrand and Hurvitz, again, ignore Plaintiffs' allegations and the applicable law.

Defendants created a business intent on violating the privacy of millions of American citizens with impunity. This Court should deny their motion to dismiss so that the case can move forward, and they can be held accountable for their wrongful conduct.

## FACTUAL BACKGROUND

***The Illinois Biometric Information Privacy Act***:

BIPA prohibits a private entity from, among other things, collecting distributing a person's biometric identifiers and information without notice and consent. It also prevents an entity from trading, selling and profiting from that biometric data. *See* 740 ILCS § 14/15. Biometric identifiers include a "scan of … face geometry." 740 ILCS § 14/10. Biometric information is "any information … based on an individual's biometric identifier used to identify an individual." *Id.* In enacting BIPA, the Illinois General Assembly recognized the extreme sensitivity and unique nature of biometrics due to the fact that a person cannot change them if compromised 740 ILCS § 14/5(c).

***The Biometric Database***

Without providing notice or obtaining consent, Defendants scraped from the internet three billion photographs – including photographs of Plaintiffs – and then scanned the face geometry of each depicted individual to harvest their unique biometric identifiers and information (collectively "biometrics"). Dkt. 116 ¶¶1, 30, 53, 58-59. Defendants then created a searchable biometric database (the "Database") that allowed users to identify unknown individuals by uploading a photograph. *Id.* Defendants have, *inter alia*, distributed, sold and otherwise profited from the

biometrics they unlawfully collected. *Id.* ¶¶31, 54-56. Indeed, Defendants have made the Database available to thousands of entities, public and private – including Illinois entities. *Id.*¶¶3, 32-33.

***The Parties and Class Members***

Plaintiffs are individuals from Illinois, New York, California and Virginia who have brought statutory, constitutional and common law claims on behalf of members of a nationwide class and Illinois, California, New York and Virginia subclasses. *Id*. ¶¶5-13, 65. Photographs of Plaintiffs' faces that were taken in, and uploaded to the internet from, each Plaintiffs' state of residence are posted online. *Id.* ¶¶ 44-52. Plaintiffs allege that Defendants have included Plaintiffs' and class members' biometrics – extracted from such photographs – in the Database. *Id.* ¶¶44-52.

Clearview is a Delaware corporation that created the unlawful Database which it markets throughout the United States, including in Illinois. *Id.* ¶14. Ton-That and Schwartz co-founded Clearview and are the architects of its alleged illegal scheme. *Id.* ¶¶15-16. They are Clearview's CEO and President, respectively, and participated in, authorized and directed Clearview's wrongful acts. *Id.*; *see also id.* ¶¶37-39. Clearview, through Ton-That and Schwartz, has executed hundreds of agreements with Illinois entities and sold and profited from Plaintiffs' and class members' biometrics. *Id.* ¶¶21, 30-31.

Rocky Mountain is a New Mexico company whose single client was the Illinois Secretary of State (the "Illinois SoS") – to which it offered access to the Database. *Id.* ¶¶18, 22. Clearview was Rocky Mountain's parent and had control over and was involved in Rocky Mountain's alleged misconduct regarding the biometrics at issue, causing foreseeable injuries. *Id.* ¶43. Rocky Mountain was a corporate shell that Ton-That and Schwartz did not capitalize. *Id.* ¶41. Rocky Mountain has no employees, assets or products separate from those of Clearview. *Id.* ¶¶22, 42.

Mulcaire is Rocky Mountain's Vice President and Clearview's General Counsel. *Id.* ¶17. Through Mulcaire, Rocky Mountain fraudulently represented to the Illinois SoS that it was the sole manufacturer and provider of the Database. *Id.* ¶39. Mulcaire provided the Illinois SoS with his personal information in order to be paid for work performed by Rocky Mountain. *Id.* ¶¶17, 22.

## ARGUMENT

### I. Plaintiffs Plead Sufficient Facts to Hold the Individual Defendants Responsible for Clearview's Conduct.

Defendants claim the Individual Defendants should be "dismissed from this action because they cannot be held liable for actions they took while acting as officers and employees of Clearview." Dkt. 88 at 4.[1] As a threshold matter, Defendants make no claim that the Individual Defendants cannot be individually liable for Rocky Mountain's conduct, despite the Complaint alleging such personal liability. *See* Dkt. 116 ¶¶39-42. Thus, in all events, the Court should not dismiss the Individual Defendants from the action.

As for the Individual Defendants liability for Clearview's conduct, Defendants incorrectly frame the issue as one of veil piercing (Dkt. 88 at 4), when the issue is whether the Individual Defendants personally participated in or authorized Clearview's tortious conduct. *Brandt v. Rokeby Realty Co.,* 2004 WL 2050519, at *9 (Del. Super. Ct. Sept. 8, 2004) (emph. added). Under Illinois and Delaware law[2], the "personal participation doctrine" provides that agents of a limited liability company or corporation can be liable for torts they participated in or authorized. *See RNS Servicing, LLC v. Spirit Constr. Servs., Inc.,* 2018 WL 3729326, at *6 (N.D. Ill. Aug. 6, 2018)

[1] Defendants summarily seek dismissal of Mulcaire and Rocky Mountain, claiming lack of personal jurisdiction. Dkt. 88 at 12. The cursory argument is waived, *Crespo v. Colvin*, 824 F.3d 667, 673 (7th Cir. 2016), and ignores Rocky Mountain's and Mulcaire's ties to Illinois. Dkt. 116 ¶¶17-18, 42. The Court previously rejected the argument as to Clearview, Ton-That and Schwartz. *Mutnick* Dkt. 86.

[2] Because Delaware and Illinois law yield the same result, a choice of law analysis is not required. *LeClercq v. Lockformer Co.*, No. 00 C 7164, 2002 WL 908037, at *5 (N.D. Ill. May 6, 2002).

(applying Delaware's personal participation doctrine); *People ex rel. Madigan v. Tang*, 346 Ill. App. 3d 277, 284, 805 N.E.2d 243, 250 (2004) (corporate officer not insulated from corporation's torts in which he actively participates).

The Complaint alleges the Individual Defendants' participation in, and authorization of, Clearview's tortious conduct, subjecting them to liability for that conduct. *See, e.g.,* Dkt. 116 ¶¶15-16 (Ton-That and Schwartz knew of, authorized and directed the alleged wrongful acts and were architects of Clearview's illegal scheme to collect and distribute biometrics), 21 (Ton-That and Schwartz executed agreements on Clearview's behalf), 38 (Schwartz personally paid Clearview's expenses and received payments at his home), 39 (Ton-That and Schwartz treated the Database as their own), 37 (Ton-That and Schwartz undercapitalized Clearview).

Under an alter-ego/veil-piercing analysis, the result is the same. To state an alter ego claim, a plaintiff must allege: (a) that the corporation and its shareholders operated as a unified economic entity; and (b) the presence of an element of injustice or unfairness.[3] *Galligan v. Adtalem Global Educ. Inc.*, at *6 (N.D. Ill. Jan. 15, 2020). "Seven factors guide this analysis: (1) undercapitalization; (2) failure to observe corporate formalities; (3) nonpayment of dividends; (4) the insolvency of the corporation; (5) siphoning of the corporation's funds by the dominant stockholder; (6) absence of corporate records; and (7) the fact that the corporation is merely a façade for the operations of the dominant stockholder or stockholders." *Id.*

The Complaint alleges a "unity of interest" between Clearview and its principals that dissolved their separate personalities. Dkt. 116 ¶36. For instance, the Complaint alleges that Ton-That and Schwartz undercapitalized Clearview to shield it from paying legal obligations. *Id.* ¶37.

[3] Defendants wrongly claim that fraud is always necessary to pierce the corporate veil when, in fact, Delaware requires a showing of "fraud or similar injustice." *Mason v. Network of Wilmington, Inc.*, 2005 WL 1653954, at *3 (Del. Ch. 2005).

The Complaint also alleges a lack of corporate formalities – *e.g.*, Schwartz personally funding Clearview's expenses and directing that payments be sent to his home. *Id.* ¶38. Moreover, the Complaint alleges that Clearview was a façade for Ton-That's and Schwartz's operations, as they treated Clearview's Database as their own, transferring "ownership" of it as they saw fit. *Id.* ¶39. These allegations and the corresponding inferences satisfy the elements of an alter-ego claim.

## II. The Complaint Alleges Facts Sufficient to Pierce Rocky Mountain's Corporate Veil.

Defendants' contention that Plaintiffs have failed to pierce Rocky Mountain's corporate veil (Dkt. 88 at 13) similarly fails. To hold a parent company liable for the actions of a subsidiary, the corporate veil must be pierced. *See StrikeForce Techs., Inc. v. PhoneFactor, Inc.,* 2013 WL 6002850, at *3 (D. Del. Nov. 13, 2014) (as amended).[4] The corporate veil may be pierced under an alter ego test or an agency test. *Id.* Plaintiffs described the alter ego test above. *See id.* Under the agency theory, a parent is liable for the specific conduct it directed, authorized, or instigated the subsidiary to perform. *Id.* at 5.

Here, Rocky Mountain's corporate veil may be pierced under both tests. Under the agency theory, Plaintiffs have alleged Clearview (through the Individual Defendants) was responsible for Rocky Mountain's unlawful conduct with respect to Plaintiffs' and class members' biometrics – namely, the collection, use, distribution and sale of the biometrics. Dkt. 116 ¶¶39, 43.

Plaintiffs' allegations also satisfy both requirements of the alter-ego test. First, Plaintiffs have alleged inattention to corporate formalities, such as: (a) a Clearview employee (paid by Clearview) posing as a Rocky Mountain employee; (*id.* ¶42); (b) Mulcaire seeking personal payment for Rocky Mountain's work (*id.*); and (c) Clearview allowing Rocky Mountain to fraudulently represent that the Database was its own "proprietary technology" (*id.* ¶ 39). These

[4] When determining a Delaware parent company's liability for the actions of a subsidiary, courts routinely apply Delaware law. *See, e.g., Mobil Oil Corp. v. Linear Films, Inc.,* 718 F. Supp. 260, 267 (D. Del. 1989).

allegations support the reasonable inference that Rocky Mountain was merely a façade of Clearview that was dominated and controlled by Clearview (through the Individual Defendants).

Second, use of the corporate form would result in an injustice. As Defendants admit, Rocky Mountain was a corporate shell that was not capitalized at all. *Id.* ¶ 41; Dkt. 88 at 13 (Rocky Mountain has "no actual operations"). Given that Rocky Mountain only did business with an Illinois entity (*see* Dkt. 116 ¶¶17-18), it is reasonable to infer that by failing to capitalize Rocky Mountain, Clearview attempted to distance itself from BIPA liability while making Rocky Mountain judgment proof.

**III. Plaintiffs Have Sufficiently Pled Their Claims Against Rocky Mountain.**

Defendants' contention that Plaintiffs fail to sufficiently allege claims against Rocky Mountain (Dkt. 88 at 13-14) ignores the Complaint's Rocky Mountain-related allegations (as described above), which are incorporated into Plaintiffs' claims against Rocky Mountain. *See* Dkt. 116 ¶¶17-18, 22, 39-43, 90, 105, 119, 126, 134, 150, 163, 170, 177, 184, 193, 201. Properly considered, the Complaint's allegations state claims against Rocky Mountain.

**IV. Plaintiffs' BIPA Claims Do Not Violate the Extraterritoriality Doctrine.**

Defendants incorrectly contend that Plaintiffs' BIPA claims violate Illinois' extraterritoriality doctrine. Dkt. 88 at 14-15. As a threshold matter, Defendants do not claim that Plaintiffs' Rocky Mountain-based BIPA claims in Counts Two, Four and Six violate the doctrine, nor could they, given that the sole transaction at issue in those counts was in Illinois with an Illinois customer. Dkt. 116 ¶¶22, 39, 42. Moreover, as to Rocky Mountain, that was its singular transaction.

With respect to Plaintiffs' remaining BIPA claims, courts considering Defendants' contention in a similar BIPA context have routinely rejected it as premature at the Rule 12(b)(6) stage. *See, e.g., Patel v. Facebook*, Inc., 932 F.3d 1264, 1275-76 (9th Cir. 2019); *Vance v. Int'l*

*Business Machines Corp.*, 2020 WL 5530134, at *3 (N.D. Ill. Sept. 15, 2020); *Rivera v. Google*, Inc., 238 F.Supp.3d 1088, 1100-02 (N.D. Ill. 2017); *Monroy v. Shutterfly*, Inc., 2017 WL 4099846, at *5-7 (N.D. Ill. Sept. 15, 2017); *see also see Morrison v. YTB Intern., Inc.*, 649 F.3d 533, 538 (7th Cir. 2011) (only extraordinary circumstances justify dismissal on extraterritoriality grounds at Rule 12(b)(6) stage). This is because application of the extraterritoriality doctrine requires a fact-intensive inquiry. *Avery v. State Farm Mut. Auto. Ins. Co.,* 835 N.E.2d 801, 854 (Ill. 2005).

On the merits, Defendants view Plaintiffs' allegations in an improper light and assert Plaintiffs fail to allege facts showing their claims occurred primarily and substantially in Illinois. Dkt. 88 at 15. Properly considered, Plaintiffs' allegations raise a question of fact as to whether the BIPA claims occurred primarily and substantially in Illinois. In *Avery*, the relevant circumstances occurred "primarily and substantially" in the situs where, among other things: (a) plaintiffs resided; (b) the deception or "failure to disclose" occurred; and (c) the plaintiffs incurred their injury.[5] *Id.* at 854. Here, each of those relevant circumstances occurred in Illinois: (a) Illinois subclass members are Illinois residents (Dkt. 116 ¶65); (b) Defendants failed to provide notice to the Illinois subclass members in Illinois (*see id.* ¶58); and (c) Defendants trespassed on Illinois subclass members' private domains in Illinois. *See Bryant v. Compass Group USA, Inc.*, 958 F.3d 617, 624 (7th Cir. 2020). Moreover, Defendants contracted with hundreds of Illinois entities (Dkt. 116 ¶20), and it is reasonable to infer Clearview created Rocky Mountain as a judgment-proof entity that would transact business in Illinois.

That Clearview is headquartered in New York (*see* Dkt. 88 at 15) does not change the above analysis. *See Avery*, 835 N.E.2d at 854-55 (defendant's home state does not control);

[5] *Avery* addressed extraterritoriality in the context of Illinois' Consumer Fraud Act and required that "the circumstances *that relate to disputed transactions* occur primarily and substantially in Illinois." *Avery*, 835 N.E.2d at 854 (emph. added). Because BIPA regulates different conduct, the circumstances that must occur primarily and substantially in Illinois likely are different.

*Landau v. CNA Fin. Corp.*, 886 N.E.2d 405, 407-09 (Ill. App. Ct. 2008) (cited by Defendants) (same); *Phillips v. Bally Total Fitness Holding Corp.*, 865 N.E.2d 310, 315-16 (Ill. App. Ct. 2007) (cited by Defendants) (same). Similarly, the fact that Defendants collected and distributed the biometrics of non-Illinois residents (Dkt. 88 at 15) has no bearing on the above analysis, which focuses on Defendants' conduct vis-à-vis Illinois subclass members asserting BIPA claims.

*Vulcan Golf, LLC v. Google Inc.,* 552 F.Supp.2d 752 (N.D. Ill. 2008) (Dkt. 88 at 15, n.4), is distinguishable. Unlike here, the complaint in that case contained "*no allegations* that plausibly suggest that the purported deceptive domain scheme occurred primarily and substantially in Illinois." *Vulcan Golf, LLC*, 552 F.Supp.2d at 775 (emph. added).

**V. The Dormant Commerce Clause Does Not Apply to Plaintiffs' BIPA Claims.**

Dismissal on dormant Commerce Clause grounds (*see* Dkt. 88 at 15-17) is similarly premature. In the BIPA context, courts have routinely rejected dormant Commerce Clause challenges, especially at the Rule 12(b)(6) stage. *See, e.g., In Re Facebook Biometric Info. Privacy Litig.*, 2018 WL 2197546, at *4 (N.D. Cal., May 14, 2018); *Vance*, 2020 WL 5530134, at *3-4; *Rivera*, 238 F.Supp.3d at 1102-04; *Monroy*, 2017 WL 4099846, at *7-8.

Notably, the dormant Commerce Clause does not apply here because it only "precludes the application of a state statute to commerce that takes place *wholly* outside of the State's borders, whether or not the commerce has effects within the state." *Rivera*, 238 F.Supp.3d at 1103 (quoting *Healy v. Beer Inst., Inc.,* 491 U.S. 324, 336 (1989)) (internal quotation marks omitted) (emph. added). As discussed above, Plaintiffs allege substantial conduct that occurred in Illinois.

New York's failure to enact biometric legislation (*see* Dkt. 88 at 16) is of no import. New York may expose its residents to biometric privacy harms, while Illinois is free to protect its residents from them. Unlike in *Morley-Murphy Co. v. Zenith Elecs. Corp.*, 142 F.3d 373, 379 (7th

Cir. 1998), and *Midwest Title Loans, Inc. v. Mills*, 593 F.3d 660, 668 (7th Cir. 2010) (Dkt. 88 at 16-17), applying BIPA in this case would not "stymie[]" or "trump" the legislative choices of states that have opted for less regulation or "exalt the public policy of one state over that of another."[6] In actuality, Defendants seek to impose New York's regulatory scheme on Illinois, which is improper. *See Healy*, 491 U.S. at 337. A different conclusion would allow any company to violate Illinois residents' biometric privacy merely by using computers outside of Illinois to collect the data. The dormant Commerce Clause does not contemplate such a perverse result.

Defendants' claim that Illinois residents only make up "some small percentage" of the Database (Dkt. 88 at 17) is not alleged in the Complaint and otherwise views the pleadings in an improper light. Moreover, Defendants cite no authority: (a) for the proposition that Illinois can only protect Illinois residents over a certain threshold; or (b) prohibiting a state from protecting its residents from tortious conduct if the tortfeasor also harms people elsewhere. On Defendants' theory, a state's tort law could never apply to in-state harms inflicted by large corporations.

Defendants' contention that BIPA precludes it from collecting *any* online photographs because it is "impossible" to determine where a photo subject resides (Dkt. 88 at 17) is not based on the Complaint's allegations. Further, BIPA regulates biometrics, not photographs. *See* 740 ILCS 14/15. Notably, BIPA is not a strict liability statute. *See* 740 ILCS 14/20. Defendants must only make reasonable efforts to identify Illinois residents. Their refusal to do so does not create a dormant Commerce Clause issue.

Defendants' citations to out-of-circuit dicta about the Internet from cases between 1997 and 2003 (see Dkt. 88 at 16 n.6) are inapposite. The modern view is that states can regulate online conduct involving their citizens without offending the dormant Commerce Clause. *See S.*

[6] *Midwest Title* is also distinguishable because it involved an Indiana statute that, unlike BIPA, sought to impose Indiana licensing requirements on transactions executed by both parties out of state. *Id.* at 662-63.

*Dakota v. Wayfair, Inc*., 138 S.Ct. 2080, 2097-2100 (2018) (in modern times, it is no longer appropriate to use the dormant Commerce Clause to "limit[] the lawful prerogatives of the States" by requiring that regulated entities have a physical presence). So too here: through BIPA, Illinois is exercising its sovereign prerogative to protect the privacy of its citizens.

## VI. The First Amendment Does Not Bar Plaintiffs' BIPA Claims.

Defendants' contention that the First Amendment bars Plaintiffs' BIPA claims (Dkt. 88 at 17-25) lacks merit. Laws that regulate conduct do not implicate the First Amendment merely because a party wishes to use the regulated conduct in service of some future speech. *See Rumsfeld v. Forum for Academic. & Inst'l Rts., Inc.,* 547 U.S. 47, 66 (2006). Rather, a First Amendment injury only arises if the regulated conduct is "so inherently expressive" that it warrants constitutional protection. *Id.* at 47. Under those circumstances, the challenged regulation is subject to intermediate scrutiny and is constitutional if "it furthers an important or substantial governmental interest; if [that] interest is unrelated to the suppression of free expression; and if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest." *U.S. v. O'Brien*, 391 U.S. 367, 377 (1968).

Because collecting and using a person's private data is conduct – not speech – laws that regulate such collection and use do not implicate the First Amendment. *See Dahlstrom v. Sun-Times Media*, LLC, 777 F.3d 937, 947 (7th Cir. 2015). If a challenged law directly regulates speech, a court must consider whether it does so in a content-neutral or content-based manner. *Id.* at 950. Intermediate scrutiny applies to content-neutral regulations. *Id.* at 949, 952.

### A. BIPA Regulates Conduct – *i.e.*, the Collection and Use of Private Information.

BIPA regulates the collection and use of a person's sensitive and private biometrics. *See* 740 ILCS 14/5 and 15; *see also See Bryant*, 958 F.3d at 624 (referring to biometrics as "private

information"); *Patel*, 932 F.3d 1264, 1273 ("using facial-recognition technology without consent . . . invades an individual's private affairs"). As such, BIPA is similar to many regulations that safeguard from misuse various categories of private or confidential information.[7]

Yet, Defendants assert that a person's sensitive biometrics are somehow "public information" because they can be harvested from photographs. Dkt. 88 at 11-12. The private nature of biometric data is not transformed into public information simply because technology has made it easier to obtain from public sources. It is well-settled that limitations exist on "the power of technology to shrink the realm of guaranteed privacy." *See Kyllo v. United States*, 533 U.S. 27, 34 (2001) (home still private despite technology that can peer inside). For instance, the Supreme Court has held that individuals retain a privacy interest in their sensitive personal information even though such information can be reconstructed from pieces of data they have made visible to others. *See Carpenter v. United States*, 138 S.Ct. 2206, 2219–20 (2018). In *Carpenter*, the Court held that individuals do not passively surrender their privacy interest in their physical movements or locations merely because in modern society "there is no way to avoid leaving behind a trail of location data." *Id.* Similarly, individuals do not surrender their biometric privacy interest merely because they cannot avoid having images posted online from which their biometrics may extracted.

Defendants' cited authority regarding publicly-posted or -filed information (Dkt. 88 at 20 and n.9) is inapposite. While Defendants try to paint a picture of a company that simply gathers publicly-available photographs and stores them in a database (*see, e.g., id.* at 19), that is not the case. This case is *not* about Defendants' collection of online photographs. It is about Defendants'

[7] *See, e.g.,* Children's Online Privacy Protection Act of 1998 ("COPPA"), 15 U.S.C. § 6501, *et seq.* (children's personal information); Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. § 1320d, *et seq*. (patient health records); Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681 (credit records); Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. § 1232g (school records); Illinois Genetic Information Privacy Act, 410 ILCS 513/1, *et seq.* (genetic information).

trespass on the private domains of millions of Americans by harvesting their unique and immutable biometrics for personal gain.[8] It is this non-public and personal biometric data that underlies Defendants' business model. *See* Dkt. 116 ¶¶1-2. And it is this non-public biometric data that allows Defendants to identify otherwise unidentifiable people. BIPA regulates this non-public data.

Notably, Plaintiffs allege that Defendants harvest the non-public biometric data from images posted online (*id.* ¶1), regardless of who posted the photograph. The cases cited by Defendants for the proposition that a person has no expectation of privacy in photographs he or she posts online (Dkt. 88 at 20) do not apply to an image of an individual posted by someone else.

**B. There is No First Amendment Right to Access or Use Private Information.**

Because BIPA regulates conduct, it cannot give rise to a First Amendment injury. *Dahlstrom* is instructive. There, the court held that a "limitation on obtaining personal information [from driving records] is *not a restriction on speech at all*" and did not trigger any First Amendment scrutiny. *Dahlstrom,* 777 F.3d at 949 (emph. added). According to the court, "a limitation only on access to information" cannot by itself allow the party desiring the information to claim a First Amendment injury. *Id*. at 947. The First Amendment does not provide an "expansive right to gather information," even for the press. *Id.* at 946. A different conclusion would endanger the constitutionality of a wide range of permissible privacy statutes. *Id.* at 947.

Other courts upholding privacy statutes against First Amendment challenges have relied on reasoning similar to that in *Dahlstrom*. *See, e.g., United States v. Miami University*, 294 F.3d 797, 820-24 (6th Cir. 2002) (rejecting First Amendment challenge to FERPA – press does not have

[8] Even if biometrics extracted from public photographs were "public information," the government is entitled to regulate the use of that information to protect privacy, just as the federal government regulates the use of publicly-available telephone numbers through the "Do Not Call List" and the Telephone Consumer Protection Act. *See, e.g., Nat'l Coalition Of Prayer, Inc. v. Carter*, 455 F.3d 783, 790 (7th Cir. 2006); *Mainstream Mktg. Servs., Inc.* v. FTC, 358 F.3d 1228, 1223 (10th Cir. 2004).

a "constitutional right of special access to information not available to the public generally"); *Offor v. Mercy Med. Ctr.*, 167 F.Supp.3d 414, 445 (E.D.N.Y. 2016), *vacated in part on other grounds*, 676 F. App'x 52 (2d Cir. 2017) (collecting cases – "information protected by HIPAA is not subject to a First Amendment or common-law right of access" even in otherwise public court documents).

Defendants' cited authority does not establish a First Amendment right to collect or use private information or that such conduct constitutes speech. Citing *Sorrell v. IMS Health*, 564 U.S. 552 (2011), Defendants argue that BIPA "violates the First Amendment by inhibiting Clearview's ability to collect, analyze, and include [] public information in its product." Dkt. 88 at 19. But *Sorrell* does not preclude Illinois from designating biometrics as private or regulating their collection and use. In that case, the Court held that a Vermont statute that prohibited pharmacies from providing physician prescriber-identifying data to marketers, but not to others, violated the First Amendment by imposing content and speaker-based restrictions. *Id.* at 580. According to the Court, Vermont did *not* treat the information at issue as private or attempt to protect it from disclosure more generally. *Id.* at 573. Instead, the state "made prescriber-identifying information available to an almost limitless audience" except for the specifically disfavored speakers. *Id.* The Court noted that "the State might have advanced its asserted privacy interest by allowing the information's sale or disclosure in only a few narrow and well-justified circumstances." *Id*.

BIPA is unlike the Vermont statute and more akin to HIPAA, which the Court cited approvingly in *Sorrell. Id.* at 580. BIPA uniformly limits access to and the use of biometrics without informed consent except for "a few narrow and well-justified circumstances." *Sorrell* thus supports BIPA's constitutionality.

### C. The Regulated Conduct Is Not Sufficiently Expressive to Implicate the First Amendment.

Nothing about the conduct at issue here is "so inherently expressive" that it qualifies for First Amendment protection. *See Rumsfeld*, 547 U.S. at 49. Just as a newspaper's collection of private information to publish a news story does not constitute protected expression, *see Dahlstrom*, 777 F.3d at 947, 949, neither does Defendants' conduct here.

Defendants' non-binding authority from the early 2000s (Dkt. 88 at 19) does not change this analysis. In *Search King, Inc. v. Google Tech, Inc.*, 2003 WL 21464568 (W.D. Okla. May 27, 2003), the court held that a search engine's ranking of public websites was protected First Amendment opinion. *Id.* at *4. Unlike here, the case did not involve the collection and use of private data. At issue in *Junger v. Daley*, 209 F.3d 481 (6th Cir. 2000), was the publication of a professor's source code. *Id.* at 484. Here, the biometrics belong to Plaintiffs and class members, and Defendants did not create or "write" those biometrics.

### D. Even If BIPA Burdens Speech, It Is Subject to Intermediate Scrutiny.

When a challenged statute regulates speech, "[t]he appropriate standard of review for such a regulation hinges on whether the regulation is content based, which requires [the court] to apply strict scrutiny, or content neutral, which demands only an intermediate level of scrutiny." *Dahlstrom*, 777 F.3d at 949.[9] A statute is content-based if it: (a) restricts "particular viewpoints"; or (b) targets "public discussion of an entire topic" or "subject matter" for differential treatment. *Reed v. Town of Gilbert*, 576 U.S. 155, 168-69 (2015).

[9] The *Dahlstrom* decision treated that privacy statute's dissemination provision as a content-neutral speech regulation that withstood intermediate scrutiny. 777 F.3d at 949. It found the statute's information-collection provision to be a regulation of conduct. *Id.* If the Court determines BIPA § 15(d) to be a speech regulation, it is similarly content-neutral and permissible under intermediate scrutiny. *See infra.*

To the extent BIPA burdens speech by regulating the dissemination of biometrics without notice and consent, it does so in a content-neutral manner and is, therefore, subject to intermediate scrutiny. Illinois enacted BIPA to protect its residents' biometric privacy, not because it agreed or disagreed with any message communicated by individuals' biometrics. *See* 740 ILCS 14/5. Moreover, BIPA neither restricts particular viewpoints nor targets public discussion of an entire topic or subject matter for differential treatment. *Cf. Sorrell*, 564 U.S. at 564, 566. BIPA requires a private entity to receive informed consent before obtaining and using individual's biometrics no matter what sort of "speech" or content it wishes to express once it possesses those biometrics. Rather than burdening any particular speech content, BIPA permissibly protects sensitive private information. *Cf. State of Ill. v. Austin,* 155 N.E.3d 439, 458 (Ill. 2019) ("The entire field of privacy law is based on the recognition that some types of information are more sensitive than others . . . ").

BIPA's content-neutral nature is underscored by Defendants' strained effort to transform it into a content-based regulation. *See* Dkt. 88 at 21-23. According to Defendants, BIPA "targets attempts to identify people that it deems too dangerous (from a privacy standpoint) merely because of their effectiveness." *Id.* at 21. To show differential treatment, Defendants hypothesize that Plaintiffs would not take issue with a process by which individuals manually sought to match photographs. *Id.* But BIPA does not target the matching of photographs – whether by hand or by automation; it regulates the collection and dissemination of biometrics. If the hypothetical people who were manually matching photographs also were collecting and disseminating biometrics, BIPA would treat them the same as anyone else, subject to expressly-stated permissible exceptions. Conversely, Defendants would be treated the same if they were *not* engaged in photograph matching. BIPA is not content-based, and strict scrutiny does not apply.

Beyond claiming that BIPA is a content-based speech restriction, Defendants claim it is a speaker-based restriction. Dkt. 88 at 22. Defendants point to two express exceptions to BIPA's regulations – *i.e.*, exceptions for employees and contractors of a "State agency or local unit of government" and certain federally-regulated financial institutions. *Id.* Strict scrutiny is only triggered for speaker-based regulations when the speaker preference "*reflects a content preference.*" *Reed*, 576 at 155 (citation omitted, emph. added); *see also Dahlstrom*, 777 F.3d at 950. If statutory exceptions may have an incidental effect on some messages or speakers, the statute remains content neutral if the exceptions' goals are unrelated to the regulated content of expression. *Dahlstrom*, 777 F.3d at 950.

BIPA's limited exceptions are unrelated to any content preference. The exception for financial institutions defers to federal law that already governs collection of private data by these entities. *See* 740 ILCS 14/25(c); 12 C.F.R. § 1016 (data privacy rule applicable to federally-regulated financial institutions). While the state agency/local unit of government exception may have some incidental effect on some speakers and not others, BIPA remains content neutral because the goals of the exception – allowing employees and contractors of a "State agency or local unit of government" to perform their public functions – are unrelated to the content of the regulated expression. *See Dahlstrom*, 777 F.3d at 950, 950 n.5 (permissible exceptions include one for "government or security entities"). Virtually all privacy regulations entrust some individuals or entities with the regulated information, but not others. *See, e.g.*, 20 U.S.C. § 1232g(b)(1)(A)–(L) (FERPA provisions designating permissible recipients). To treat every such statute as a "speaker-based" speech regulation subject to strict scrutiny would upend all of privacy law.

**E. BIPA Withstands Intermediate Scrutiny.**

Under *O'Brien*, BIPA, as applied here, withstands intermediate scrutiny. First, BIPA furthers Illinois' substantial interest in protecting residents' sensitive and immutable biometrics from unauthorized collection and dissemination. *See* 740 ILCS 14/5; *Rosenbach v. Six Flags Entn't Corp.*, 129 N.E.3d 1197, 1206 (Ill. 2019) (BIPA protects citizens' control over their highly sensitive data); *Patel*, 932 F.3d at 1274*; see also Dahlstrom*, 777 F.3d at 952. Second, Illinois' interest is unrelated to the suppression of any sort of expression and, by reducing the fear of omnipresent surveillance, BIPA promotes and protects free expression that might otherwise be chilled.

Third, any incidental restriction BIPA places on alleged First Amendment freedoms is no greater than is essential to the furtherance of Illinois' above-described interest. This "narrow-tailoring" requirement is satisfied where a regulation promotes a substantial government interest that would be less effectively achieved without the regulation. *Dahlstrom*, 777 F.3d at 954. The regulation need not be the least speech-restrictive means of advancing the state's interests. *Id.* BIPA promotes biometric privacy much more effectively than would be the case absent its regulations. BIPA achieves this interest while still allowing individuals to share their biometrics and third parties to share them with consent. *Cf. Austin,* 155 N.E.3d at 457 ("revenge porn" regulation with no liability for images obtained and distributed with consent withstood intermediate scrutiny).

As discussed above, Defendants' contention that BIPA does not protect confidential and sensitive information because the biometrics at issue are harvested from photographs available online (Dkt. 88 at 23) fails. Defendants' contention that BIPA is overbroad because it suppresses speech adults have a right to receive and disseminate (Dkt. 88 at 24-25) similarly fails. Defendants' impermissibly premise their contention on facts outside the record – *i.e.*, that they have a limited

ability to discern the residencies of subjects of online photographs. *Id.* at 25. Based on that unsupported premise, Defendants state that BIPA essentially bans their ability to match publicly-available photographs with other photographs. *Id.* On this undeveloped record, Defendants' contention necessarily fails. Moreover, nowhere does BIPA prevent Defendants from obtaining anyone's consent, obtaining photographs, or matching photographs with other photographs. Further, BIPA only applies to Illinois residents. Defendants are free to use photographs of residents from the rest of the world without concern for BIPA.

**VII. The Complaint Sufficiently Alleges a Violation of BIPA § 15(c).**

Ignoring the Complaint's allegations, Defendants contend it fails to allege they sold, leased, traded or otherwise profited from Plaintiffs' and Class Members' biometrics in violation of BIPA § 15(c). Dkt. 88 at 25-28. Further ignoring the Complaint's allegations, Defendants also contend that Plaintiffs incorrectly construe § 15(c)'s "otherwise profit from language" to mean "profit[ing] from technology that relies on biometrics." *Id.* at 26. The arguments lack merit.

Section 15(c) provides that "[n]o private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or customer's biometric identifier or biometric information." 740 ILCS 14/15(c). The Complaint is replete with allegations regarding Defendants' sale, lease and trade for profit of the biometrics at issue. *See, e.g.,* Dkt. 116 ¶¶2 (developed technology for profit), 31 (sold, traded, leased and otherwise profited from unlawfully collected biometrics), 32 (sold access to Database to 1000s), 33 (sold access to database to entities that queried it to identify people), 55 (distributed biometrics to private entities who obtained the biometrics contained therein), 56 (profited from the biometrics in the Database by selling them to entities). Additionally, Counts Three and Four are specifically directed at

Defendants' violations of § 15(c) as a result of their "selling, leasing, trading and otherwise profiting from individuals' biometric identifiers and biometric information." *Id.* ¶¶99, 106.

Even accepting *arguendo* Defendants' narrow interpretation of "otherwise profit from" to solely mean profiting from the transfer of a person's biometrics to another in exchange for consideration (Dkt. 88 at 26), Plaintiffs' allegations are sufficient. At minimum, Defendants transferred for profit Plaintiffs' and class members' biometric information to customers – indeed, the entire premise of Defendants' business is to provide identifying information to customers based on a person's biometric identifiers. *See* Dkt. 116 ¶55.

A court in this District recently denied a motion to dismiss based on the same § 15(c) arguments Defendants present here. *See Flores v. Motorola Sols., Inc.,* 2021 WL 232627, at *3 (N.D. Ill. Jan. 8, 2021). The court found that the plaintiffs' allegations that the defendants "develop[ed] the database by extracting biometric identifiers, compared novel images to the database images to find facial matches, and offer[ed] access to that database for a fee to law enforcement" sufficiently alleged a § 15(c) violation because "biometric data is a necessary element to Defendant's business model." *Id.* This Court should reach the same conclusion.

**VIII. BIPA Applies to Biometrics Extracted from Photographs.**

Courts have uniformly rejected Defendants' argument that BIPA exempts biometric data extracted from photographs. *See, e.g.*, *Flores*, 2021 WL 232627, at *3; *Vance*, 2020 WL 5530134, at *4; *Rivera*, 238 F. Supp 3d at 1095; *In re Facebook Biometric Privacy Litig.*, 185 F. Supp. 3d 1155, 1170–72 (N.D. Cal. 2016); *Monroy*, 2017 WL 4099846, at *3-5. This Court should, too.

As Defendants note, photographs themselves are not "biometric identifiers." *See* Dkt. 88 at 28. But a "scan of facial geometry" is a "biometric identifier." This is because the definition of "biometric identifier" neither specifies the means by which the scan is taken nor excludes

information derived from any particular source (unlike "biometric information," which contains such an exclusion). As the court in *Rivera* found, "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." 238 F.Supp 3d at 1096. Moreover, accepting Defendants' argument could also allow retinal scans and fingerprints to be captured from photographs with impunity. *See id.* at 1096; *Monroy*, 2017 WL 4099846, at *4. This Court should not be the first to adopt Defendants' dangerous reading of BIPA.

**IX. Plaintiffs Have Standing to Assert Their California, New York and Virginia Claims.**

Defendants contend that the New York, California and Virginia Plaintiffs lack standing because they have not suffered injuries to protected privacy interests or a concrete harm. Dkt. 88 at 29. Regarding Plaintiffs' protectable privacy interests, contrary to Defendants' contention, Plaintiffs' claims do not arise out of "sharing information." *See id.* As discussed above, Plaintiffs have alleged that Defendants unlawfully collected, used and distributed their biometrics, which are protected under state law. *See e.g.,* California Consumer Privacy Act of 2018, Cal. Civ. Code §1798.100 *et. seq.*; N.Y. State Tech. Law § 106-b; Va. Code Ann. § 18.2-186.3. As for Plaintiffs' injuries, Defendants misapprehend the law. The California, New York and Virginia Plaintiffs have suffered, and continue to suffer, the ongoing invasion of their right to privacy over their biometrics, a concrete injury that satisfies Article III.[10]

[10] Defendants' reliance on *In re Google, Inc. Priv. Pol'y Litig.*, at *2 (N.D. Cal. Dec. 28, 2012) (Dkt. 88 at 29), is misplaced. Unlike here, that case involved a modification to a company's privacy policies that impacted the company's customers. Defendants' reliance on *Antman v. Uber Techs., Inc.*, 2015 WL 6123054 (N.D. Cal. Oct. 19, 2015) (Dkt. 88 at 29), is inapposite. *Antman*'s holding was limited to situations where the sole claimed harm was the risk of identity theft. 2015 WL 6123054, at *11. Here, Plaintiffs allege they suffered concrete harm from Defendants' purposeful invasion of their privacy, not just the risk of identity theft. Also, the biometrics here are significantly more sensitive than the data at issue in *Antman*.

The Supreme Court's recent decision in *TransUnion, LLC v. Ramirez*, 549 U.S. _____, 2021 WL 2599472 (U.S. June 25, 2021) supports Plaintiffs' standing in this case. There, the Court found Article III standing for the plaintiffs' Fair Credit Reporting Act claims because the harm they suffered from a wrongful disclosure of false information had a "'close relationship' to harm traditionally recognized as providing a basis for a lawsuit in American courts – namely, the reputational harm associated with the tort of defamation." *Id.* at *10.

This case is analogous to *TransUnion.* The thrust of the California, New York, and Virginia Plaintiffs' claims is that without their knowledge or consent, Defendants obtained their biometrics, included the biometrics in their Database, and sold their biometrics to third parties. Dkt. 116 ¶¶33, 35, 143, 152, 164, 172, 178-80, 186. The asserted harms bear a "close relationship" to those associated with the traditionally recognized claims of tortious invasion of privacy, disclosure of private information and intrusion upon seclusion.

Defendants claim Plaintiffs' injury is not sufficiently concrete because they have not complained of economic harm, *e.g.,* the loss of money or the "serious threat of identity theft." Dkt. 88 at 29. However, Plaintiffs expressly allege that they face the threat of identity theft. Dkt. 116¶ 63. Moreover, economic harm is not necessary for standing. As the Court held in *TransUnion*, "[v]arious intangible harms can also be concrete," and highlighted "disclosure of private information" and "intrusion upon seclusion" as harms "traditionally recognized as providing a basis for lawsuits in American courts." *TransUnion*, 2021 WL 2599472, at *7; *see also Gadelhak v. AT&T Servs., Inc.*, 950 F.3d 458, 462 (7th Cir. 2020) (cited with approval in *TransUnion* – Article III standing in TCPA case based on "intrusion upon seclusion" tort).

Before *TransUnion*, the Seventh Circuit recognized that the existence of analogous common law claims supports Article III standing under BIPA. *Bryant*, 958 F.3d at 624 (comparing

BIPA violation to "an act of trespass"); *Fox v. Dakkota Integrated Sys., LLC*, 980 F.3d 1146, 1154 (7th Cir. 2020) (comparing BIPA violation to a "tortious invasion of privacy"). Defendants have not challenged Article III standing for the BIPA claims. But the conduct and harms underlying the BIPA claims are the same as those underlying the California, New York and Virginia Plaintiffs' claims. Thus, the standing analysis is identical, and Plaintiffs have Article III standing to bring Counts Eight through Fourteen – causes of action that serve to redress invasions of Plaintiffs' privacy as courts have traditionally understood such harms.[11]

**X. Plaintiffs' Sufficiently Plead Their Right of Publicity Claims.**

Primarily focused on Plaintiff Vestrand, Defendants seek dismissal of Plaintiffs' right of publicity claims alleged in Counts Eight, Eleven, Twelve and Fourteen. Dkt. 88 at 30-33. According to Defendants, Plaintiff Vestrand's California right of publicity claims fail because she has not alleged Defendants used her "likeness in advertising or merchandising." Dkt. 88 at 31. But right of publicity claims are not limited to the advertising context. They are intended to reach every commercial misappropriation of an individual's likeness. Notably, Defendants ignore: (a) § 3344(a)'s plain language, which prohibits, *inter alia*, the unconsented commodification and sale of a person's likeness[12]; and (b) the elements of a common law right of publicity claim, which do

[11] Intrusion upon seclusion is closely related to the tort of invasion of privacy. *See* Restatement (Second) of Torts § 652B (1977); *see also* Restatement (First) of Torts § 867 (1939) (a person is liable in tort if he "interferes with another's interest in not having his affairs known to others or his likeness exhibited to the public"). The claims at issue are closely related to these or other longstanding privacy torts. *See, e.g., Wiest v. E-Fense, Inc.*, 356 F. Supp. 2d 604, 612 (E.D. Va. 2005) (Va. Code. Ann. § 8.01–40 provides only Virginia remedy for invasion of privacy) (Count Eight); *Zinner v. Olenych*, 2015 WL 13721229, at *4 (E.D. Va. Dec. 24, 2015) (VCCA allows claims for "computer invasion of privacy") (Count 9); *Miller*, 159 Cal. App.4th at 1002 (statute is rooted in preventing the traditional harm of invasion of privacy) (Count 11); *White v. Samsung Elecs. Am., Inc.*, 971 F.2d 1395, n. 1 (9th Cir. 1992), *as amended* (Aug. 19, 1992) (right of publicity is a category of the right to privacy) (Count 12); *Pearce v. Manhattan Ensemble Theater, Inc.*, 2009 WL 3152127, at *8 (S.D.N.Y. Sept. 30, 2009) (N.Y. Civ. Rights Law §§50-51 protects individual's privacy "by preventing the unauthorized commercial exploitation of her personality.") (Count 14).

[12] Section 3344 imposes liability on any person who "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,

not require proof that an individual's likeness was used for advertising. *See Downing v. Abercrombie & Fitch*, 265 F.3d 994, 1001 (9th Cir. 2001) (common law elements).

Section 3344(a)'s legislative history underscores that injury inflicted by a violation is not limited to injuries from advertising: "The gist of the cause of action in a privacy case is . . . a direct wrong of a personal character resulting in injury to the feelings without regard to any effect which the publication may have on the property, business, [or ]pecuniary interest . . . . [T]he injury is mental and subjective . . . ." *Miller v. Collectors Universe, Inc*., 159 Cal.App.4th 988, 1002 (Cal. Ct. App. 2008).

Defendants cite no authority for their novel proposition that § 3344(a) is limited only to advertising claims or where property rights are at issue. While *Maloney v. T3Media*, *Inc.*, 853 F.3d 1004, 1010 (9th Cir. 2017) (Dkt. 88 at 30), acknowledges that the "core of the right of publicity is preventing merchandising of a celebrity's image without that person's consent," the case does not limit § 3344 solely to advertising claims. *Id.,* citing *Hilton v. Hallmark Cards*, 599 F.3d 894, 910 (9th Cir. 2009) (internal quotations omitted). In fact, the court in *Maloney* held that "the right of publicity seeks to prevent commercial exploitation of an individual's identity without that person's consent," *see* 853 F.3d at 1010, as Plaintiff Vestrand alleges in Counts Eleven and Twelve.

*Callahan v. Ancestry.com Inc.*, 2021 WL 783524, at *5 (N.D. Cal. Mar. 1, 2021) (Dkt. 88 at 31), is inapposite. *Callahan* does not limit § 3344(a) claims to advertising but holds that where the unauthorized use of a person's likeness does not involve a claimed endorsement or property rights, some other injury need be asserted. Here, Vestrand alleges that Defendants' conduct – scraping online photographs of her without consent, matching them to her identity using her ill-

or soliciting purchases of, products, merchandise, goods or services, without such person's prior consent" and thereby injures such person. Cal. Civ. Code § 3344 (West) (emphasis added).

gotten biometric data, and using its collection of matched photos in its product – injured her. *See* Dkt. 116. ¶¶61-65, 169, 175-76.

Defendants make the same flawed argument with respect to the Virginia and New York statutory right of publicity claims alleged in Counts Eight and Fourteen. Plaintiff Roberson alleges a violation of Virginia Code § 8.01-40(A), which prohibits the use of one's name, portrait or picture, without written consent, "for advertising purposes *or for the purposes of trade*." Va. Code § 8.01-40(A) (emph. added). Virginia follows the plain meaning rule in interpreting statutes. *See, e.g., Vaughn, Inc. v. Beck*, 554 S.E.2d 88, 90 (2001). The ordinary meaning of the word "trade" is the "business of buying and selling commodities, products, or services." *American Heritage Dictionary*, www.ahdictionary.com (last visited July 9, 2021). Thus, the statute's plain language directly supports this claim.

Moreover, "[i]n Virginia, one holds a property interest in one's name and likeness. Conversion occurs when, as here, a defendant uses another's personal property as its own and exercises dominion over it without the owner's consent." *Town & Country Props. v. Riggins*, 457 S.E.2d 356, 364 (1995) (citations omitted).

Contrary to Defendants' argument that "a 'trade purpose' exists only where an individual's name or likeness is used to promote or sell goods or services" (Dkt. 88 at 32), the Virginia Supreme Court has expressly held that, under the statute, "[u]se for 'advertising purposes' and use 'for the purposes of trade' are separate and distinct statutory concepts." *Riggins*, 457 S.E.2d at 362. The single unpublished decision cited by Defendants involved the use of an AOL screen name, not the plaintiff's "real name, portrait, or picture," and so is inapposite. *See* Dkt. 88 at 32, n.14.

Similarly, Defendant wrongly asserts that the term "purposes of trade" as used in § 51 of New York's Civil Rights Law is limited to those situations "where an individual's name or likeness

is used to promote or sell goods or services." Dkt. 88 at 32. *See Lerman v. Flynt Distrib. Co.*, 745 F.2d 123, 131 (2d Cir. 1984) ("purposes of trade" distinguishes the "commercialization" of a person's name or likeness from "the dissemination of news or information," as in news reporting).

Defendants' reliance on the First Amendment to avoid right-of-publicity liability (Dkt. 88 at 32-33) fails. Defendants premise their argument on facts not alleged in the Complaint – namely, that Defendants gathered Plaintiffs' photographs for some public interest purpose. *See id.* As alleged, Defendants gathered the photographs to build a Database from which they could profit. *See* Dkt. 116 ¶¶2-3, 32-33, 56-57. Because the alleged purpose of Defendants' conduct has nothing to do with public affairs, Defendants' cited cases (Dkt. 88 at 32-33) are inapposite.

**XI. Count Nine States a Claim for Violations of the Virginia Computer Crimes Act.**

Defendants contend the Virginia Computer Crimes Act ("VCCA") "is a *criminal* anti-hacking statute intended to target malicious computer break-ins." Dkt. 88. at 36 (emph. in orig.). Not so. The VCCA provides a private right of action for such violations, which need not be malicious per the statute's text. *See* Va. Code § 18.2-152.12(A).

Defendants next contend that the nonconsensual use of Roberson's pictures did not constitute "an actual injury or legally cognizable damages." Dkt. 88 at 37. As noted above, Virginia recognizes a property interest in one's name and likeness, and Defendants' conduct meets Virginia's definition of conversion. *Riggins*, 457 S.E.2d at 363. Defendants' nonconsensual conversion of Roberson's likeness resulted in her alleged injuries and damages. *See* Dkt. 116 ¶¶61-64 (injuries and damages), 134 (incorporating ¶¶1-76).

Defendants also assert that the Complaint "fails to allege that Clearview used any computer or computer network '*without authority*.'" Dkt. 88 at 37 (emph. in orig.). Again, Defendants ignore the VCCA's text. A person "uses" a computer when, *inter alia*, he causes a computer

network to "perform or to stop performing computer operations," and does so "without authority" when he "knows or reasonably should know that he has no right, agreement, or permission or acts in a manner knowingly exceeding such right, agreement, or permission." Va. Code § 18.2-152.2. Here, Plaintiff Roberson alleges Defendants used computers to perform operations (*i.e.*, scraping her computer images and extracting biometrics) they had no right, agreement or permission to perform (especially given the lack of written consent required by Code § 8.01-40(A), and the violations of the terms of service of the source websites). *See* Dkt. 116 ¶¶141, 143, 145, and 147.

Defendants also assert Plaintiff Roberson "fails to allege false pretenses, conversion, artifice, trickery, or deception." *See* Dkt. 88 at 37. This assertion is at odds with the Complaint and with Virginia law. Count Nine expressly alleges the conversion of property, which is defined under the VCCA to include "computer data" and "all other personal property regardless of whether they are tangible or intangible." Dkt. 116 ¶¶139-141 (citing Va. Code § 18.2-152.2, 152.3). That definition includes Defendants' conversion of the intangible property interest in Plaintiff Roberson's name and likeness. *See Riggins*, 457 S.E.2d at 363. Virginia also recognizes fraudulent concealment as a distinct species of fraud. *See Metrocall of Delaware v. Continental Cellular Corp.*, 437 S.E.2d 189 (1993), citing *Clay v. Butler*, 112 S.E. 697 (Va. 1922)).[13] Finally, Defendants fail to address the claim that they committed computer trespass by making an

[13] Given the substantive differences between the VCCA and the federal Computer Fraud and Abuse Act ("CFAA"), and the distinct species of property right in name or likeness recognized in Virginia, Defendants' citation to *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 999-1000 (9th Cir. 2019), is distinguishable. Further, the recent Supreme Court decision on the scope of the CFAA does not apply here. *Cf. Van Buren v. United States,* __ U.S. __, 141 S. Ct. 1648, 1659-60 (June 3, 2021) (interpreting the phrase "access a computer without authorization" in the CFAA in light of the statute's focus on "preventing the typical consequences of hacking"). The VCCA, unlike the CFAA, imposes liability for *using* a computer (including one's own) to commit acts for which one does not have authorization. *See* Va. Code § 18.2-152.12(A), (E). *Cf. Brewer v. Commonwealth,* 838 S.E.2d 557, 562 (2020).

unauthorized copy of computer data (*i.e.*, the images and associated biometrics) in violation of Virginia Code § 18.2-152.4(A)(6). *See* Dkt. 116 ¶¶144-145.

**XII. Count Ten Sufficiently Alleges a California Unfair Competition Claim.**

Defendants claim Plaintiff Vestrand lacks standing to pursue her California Unfair Competition Law ("UCL") claim because she "did not pay money to Clearview, or lose money or property due to Clearview's conduct." Dkt. 88 at 35. But Vestrand explicitly pleads an injury in fact and lost money and property. Dkt. 116 ¶161. Notably, lost money is but one way a plaintiff can establish economic injury for UCL standing. As the California Supreme Court has held, "[t]here are innumerable ways in which economic injury from unfair competition may be shown. A plaintiff may (1) surrender in a transaction more, or acquire in a transaction less, than he or she otherwise would have; (2) have a present or future property interest diminished; (3) be deprived of money or property to which he or she has a cognizable claim; or (4) be required to enter into a transaction, costing money or property, that would otherwise have been unnecessary." *Kwikset Corp. v. Superior Ct*., 51 Cal.4th 310, 323 (Cal. 2011). The "quantum of lost money or property" alleged is sufficient if it "would suffice to establish injury in fact and it suffices to allege some specific, identifiable trifle of injury." *Law Ofcs. of Mathew Higbee v. Expungement Assistance Servs.*, 214 Cal.App.4th 544, 561 (Cal. Ct. App. 2013) (internal quotations omitted).

Here, Plaintiff alleges that she is "likely to withdraw from biometric-facilitated transactions and other facially-mediated electronic participation" Dkt. 116 ¶64. This is a specific, identifiable injury with inherent economic consequences. As these types of technologies proliferate, increased costs to Plaintiffs to avoid biometrically-mediated transactions is all but certain. Those costs

themselves would be entirely avoidable to Plaintiffs but for Defendants' conduct. As such, Vestrand has alleged an injury in fact for UCL standing.[14]

**XIII. Count Thirteen Sufficiently Alleges a California Constitutional Privacy Claim.**

Defendants' bases for dismissing Plaintiff Vestrand's California Constitutional claims (Count Thirteen) lack merit. Contrary to Vestrand's allegations (*see* Dkt. 116 ¶178), Defendants assert that her claim fails because she "has not alleged that Clearview collected and misused extremely personal and sensitive information[.]" Dkt. 88 at 34. When the Complaint's allegations are considered, the assertion fails.

Again ignoring Vestrand's allegations (Dkt. 116 ¶¶24-33), Defendants claim she cannot claim a reasonable expectation of privacy in any "publicly-posted photographs." Dkt. 88 at 34. But Vestrand has pleaded that Defendants obtained the subject biometrics by covertly scraping photographs depicting her and used computers to extract her unique facial geometry. Dkt. 116 ¶¶25-33.[15] Neither Vestrand, nor anyone else, could have reasonably expected that someone would have the means or motive to obtain her biometrics from any online photographs in which she ever appeared, especially given that Defendants did so covertly and without her consent. *See Kyllo*, 533 U.S. 27 at 34 (thermal imaging camera infringed on reasonable expectation of privacy).

Finally, Defendants claim that Vestrand cannot establish an egregious breach of social norms because courts refuse to characterize "the dissemination of personally identifying information as 'egregious violations.'" Dkt. 88 at 34. Not so. The information disseminated here is categorically more serious than other personal identifying information. *See Fox*, 980 F.3d at

[14] Defendant also incorrectly contends Plaintiff fails to adequately allege predicate acts. Dkt. 88 at 35. Those predicate acts are alleged in Counts Eleven through Thirteen, as discussed herein.

[15] Defendants' reliance on *Moreno v. Hanford Sentinel, Inc.*, 172 Cal. App. 4th 1125, 1129 (2009) (Dkt. 116 34) is misplaced. Unlike the social media post of an unaltered journal entry in that case, the biometrics here are indiscernible to a viewer of the source photographs and are only revealed – not republished – by use of sophisticated and invasive technology.

1155 ("sensitivity" of immutable biometrics distinguishes them from other information). Further, despite Defendants' contention (Dkt. 88 at 35), Vestrand did not voluntarily disclose her biometrics by appearing in online photographs that she may or may not have posted.

**XIV. Plaintiffs State Claims for Unjust Enrichment**

Defendants' challenge to Plaintiffs' unjust enrichment claims (Dkt. 88 at 38-39) is meritless. As to California law, while it is "unsettled on the availability of a cause of action" for unjust enrichment, *ESG Cap. Partners, LP v. Stratos*, 828 F.3d 1023, 1038 (9th Cir. 2016) (citing cases on both sides), even cases finding no such cause of action recognize an essentially identical one for restitution, where (*inter alia*) the "defendant obtained a benefit from the plaintiff by fraud, duress, conversion, or similar conduct," *Durell v. Sharp Healthcare*, 183 Cal. App. 4th 1350, 1370 (Cal. Ct. App. 2010). Defendants obtained such a benefit here. Defendants' arguments as to Virginia and Illinois law rely on their incorrect contentions that no legal violations have been alleged, and so fail. (Defendant also cites no authority for the proposition that it did not enrich itself at Plaintiff's "expense or loss" given Plaintiffs' lost privacy.) Finally, the New York claim is not preempted by or duplicative of the right of publicity claim, given the allegations in the Complaint. *See*, *e.g.,* Dkt. 116 at ¶195 (harvested biometrics were an unjustly obtained benefit).

**XV. Plaintiffs State a Claim for Declaratory Judgment or Injunctive Relief.**

Defendants' attacks on Plaintiffs' claims for declaratory judgment and injunctive relief rest wholly on its incorrect contention that Plaintiffs fail to state a claim, and so should be rejected.

**CONCLUSION**

For the foregoing reasons, the Court should deny Defendants' motion to dismiss in its entirety. To the extent the Court grants any portion of the motion, Plaintiffs respectfully request that the denial be without prejudice and with leave to replead.

Dated: July 9, 2021

Respectfully submitted,

By: /s/ Scott R. Drury
SCOTT R. DRURY
*Interim Lead Class Counsel for Plaintiffs*

Mike Kanovitz
Scott R. Drury
Andrew C. Miller
**LOEVY & LOEVY**
311 N. Aberdeen, 3rd Floor
Chicago, Illinois 60607
312.243.5900
drury@loevy.com

Scott A. Bursor
Joshua D. Arisohn
**BURSOR & FISHER, P.A.**
888 Seventh Avenue
New York, NY 10019
646.837.7150
scott@bursor.com
jarisohn@bursor.com

Frank S. Hedin (to be admitted *pro hac vice*)
**HEDIN HALL LLP**
Four Embarcadero Center, Suite 1400
San Francisco, California 94104
415.766.3534
fhedin@hedinhall.com
Michael Drew
**NEIGHBORHOOD LEGAL LLC**
20 N. Clark Street #3300
Chicago, Illinois 60602
312.967.7220
mwd@neighborhood-legal.com

Michael Wood
Celetha Chatman
**COMMUNITY LAWYERS LLC**
20 N. Clark Street, Suite 3100
Chicago, Illinois 60602
312.757.1880
mwood@communitylawyersgroup.com
cchatman@communitylawyersgroup.com

Steven T. Webster
Aaron S. Book
**WEBSTER BOOKK LLP**
300 N. Washington, Ste. 404
Alexandria, Virginia 22314
888.987.9991
swebster@websterbook.com

*Other Counsel for Plaintiffs*

**CERTIFICATE OF SERVICE**

I, Scott R. Drury, an attorney, hereby certify that, on July 9, 2021, I filed the foregoing document using the Court's CM/ECF system, which effected service on all counsel of record.

/s/ Scott R. Drury
*Interim Lead Class Counsel for Plaintiffs*