IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS

AMERICAN CIVIL LIBERTIES UNION, et al., Plaintiffs, v. CLEARVIEW AI, INC., a Delaware corporation, Defendant.	)	No. 2020 CH 04353 Hon. Pamela Meyerson

DEFENDANT'S MEMORANDUM OF LAW
IN SUPPORT OF ITS MOTION TO DISMISS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

OTHER AUTHORITIES

Defendant Clearview AI, Inc. ("Clearview") respectfully submits this memorandum of law in support of its motion to dismiss the Complaint.

INTRODUCTION

Clearview assists law enforcement agencies in identifying perpetrators and victims of crime. Clearview collects publicly-available images from the Internet, analyzes them, and returns search results to licensed users of Clearview's service. Before Plaintiffs launched this litigation, Clearview adopted a series of voluntary business changes that ensured that the Illinois Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1 *et seq*., would not apply to Clearview's operations, thus mooting this litigation, which seeks only injunctive relief. Specifically, Clearview has instituted several technical measures designed to avoid collecting photographs from the Internet that may have originated in Illinois. In addition, Clearview has cancelled all contracts with private entities, including all entities in Illinois, and now licenses its technology only to government entities. Ex. A ¶ 16.[1] As a result of these voluntary changes, Clearview plainly is exempt from BIPA. Notwithstanding that, Plaintiffs continue to pursue injunctive relief against Clearview. The Complaint should be dismissed for the following independent reasons.

First, Clearview is not subject to personal jurisdiction in Illinois. Clearview is a small technology company incorporated in Delaware and with its principal place of business in New York. Plaintiffs' members reside in Illinois, but Plaintiffs do not allege that they have ever interacted with Clearview (in Illinois or otherwise) or that Clearview's conduct was in any way directed at them in Illinois. Plaintiffs also allege that Clearview had contracts with third parties in Illinois, but Plaintiffs' alleged injuries have nothing to do with those contracts, and in any event,

[1] Ex. A is the May 6, 2020 Declaration of Thomas Mulcaire, which was filed in *Mutnick v. Clearview AI, Inc.,* No. 20-512 (N.D. Ill.).

all of those contracts have been cancelled. Because Plaintiffs fail to allege a nexus between Clearview, Illinois, and Plaintiffs' alleged injuries, Clearview is not subject to jurisdiction here.

Second, even if Clearview were subject to jurisdiction in Illinois, the Complaint would still fail as a matter of law because Plaintiffs improperly attempt to apply BIPA to Clearview's out-of-state conduct in violation of Illinois's extraterritoriality doctrine. Under Illinois Supreme Court precedent, Plaintiffs must allege that the conduct at issue occurred "primarily and substantially" in Illinois. *Avery v. State Farm Mut. Auto. Ins. Co.*, 216 Ill. 2d 100, 186 (2005). Plaintiffs do not come close to satisfying this standard. Plaintiffs do not allege that Clearview did *anything* relevant to this case in Illinois. Accordingly, Plaintiffs' BIPA claim should be dismissed because the "majority of circumstances relating to the alleged violation" of BIPA—*i.e.*, the alleged "capturing, storing, and using" of biometric information, Compl. ¶ 73—did not occur in Illinois. *Landau v. CNA Fin. Corp.*, 381 Ill. App. 3d 61, 65 (1st Dist. 2008).

Relatedly, if BIPA were to apply to Clearview's conduct, then BIPA would violate the dormant Commerce Clause of the U.S. Constitution, which precludes the application of a state statute that has the effect of regulating conduct in another state. Unlike Illinois, New York has not passed any statutes regulating facial-recognition technology, despite considering several. In these circumstances, BIPA would be unconstitutional as applied because it would impose inconsistent obligations on Clearview and promote the public policy of Illinois over that of New York.

Third, the Complaint should be dismissed because it is barred by the First Amendment of the U.S. Constitution and Article One, Section Four of the Illinois Constitution, which protect the collection and use of public photographs that appear on the Internet.[2] All challenged acts of

[2] An Ill. Sup. Ct. R. 19 notice along with a copy of Clearview's motion and supporting papers will be served on the Illinois Attorney General.

Clearview in this case relate to its use of what the Complaint refers to as "photographs available online," Compl. ¶ 44, on Facebook and other websites, photos as to which repeated case law around the nation has held that the individuals shown have no reasonable expectation of privacy. In that context, Plaintiffs can neither survive the strict scrutiny applied in such cases or the requirement that regulations of expression must be narrowly drawn so as not to unduly limit free expression.

Fourth, the Complaint should be dismissed because the plain language of BIPA confirms that the statutory regime does not apply to Clearview's technology. Specifically, BIPA's definition of "biometric identifiers" excludes "photographs," and its definition of "biometric information" excludes "information derived from items or procedures excluded under the definition of biometric identifiers," such as photographs. 740 ILCS 14/10. Confirming that the application of facial-recognition technology to a photograph is excluded from BIPA, each of the items listed in BIPA's definition of "biometric identifiers"—"retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry," *id.*—refers to a physical, in-person process for obtaining biometric information.

For these reasons and those that follow, the Complaint should be dismissed.

BACKGROUND[3]

A. Clearview Collects Publicly-Available Photographs From New York

Clearview is a small technology company that collects publicly-available images on the Internet and organizes them into a search engine. Compl. ¶¶ 6, 54; Declaration of Richard Schwartz ("Schwartz Decl.") ¶ 4. As alleged in the Complaint, "Clearview has captured more than

[3] Without admitting any allegations against it, Clearview accepts as true the allegations in the Complaint solely for purposes of this motion. *See In re Estate of Powell*, 2014 IL 115997, ¶ 12. Moreover, the Court may consider declarations on a motion to dismiss for lack of personal jurisdiction. 735 ILCS 5/2-301; *Monahan v. CoreMedia AG*, 2015 IL App (1st) 141303-U, ¶ 42. "[T]he court must also accept as true any facts averred by the defendant which have not been contradicted by an affidavit submitted by plaintiff." *Knaus v. Guidry*, 389 Ill. App. 3d 804, 813 (1st Dist. 2009).

three billion faceprints from images available online," and through Clearview's "enormous database, it can instantaneously identify the subject of a photograph with unprecedented accuracy." Compl. ¶ 6. By using Clearview's technology, licensed law enforcement agencies and government agencies have been able to help track down at-large criminals and to identify victims of crimes. Schwartz Decl. ¶ 3.

Clearview manages its operations from its headquarters and principal place of business in New York. *Id.* ¶ 4. From locations outside of Illinois, Clearview collects photographs from the public Internet, performs a scan of facial vectors on certain of the photographs, and returns search results to licensed users of its product. *Id.* None of the servers hosting this data are in Illinois. *Id.*

B. Plaintiffs' Claims Have No Relevant Connection to Illinois

The alleged misconduct here did not occur in Illinois. Nor was it caused by actions "directed at Illinois" in any way. Plaintiffs do not allege that they have ever had any interaction with Clearview (in Illinois or otherwise) or that Clearview took any actions directed towards them in Illinois. Instead, Plaintiffs allege that: (1) Clearview "specifically marketed its services in Illinois," Compl. ¶ 62, and (2) Clearview conducts business transactions in Illinois by "actually selling its services to customers in Illinois," including to "police departments in Illinois," *id.* ¶¶ 17, 59. However, Clearview does not target Illinois through advertising or marketing. Schwartz Decl. ¶ 6. As Plaintiffs' own allegations describe, Clearview's service is used by law enforcement agencies "throughout the United States at the federal, state, and local levels." Compl. ¶ 8. With respect to Plaintiffs' allegation that Clearview contracted with parties in Illinois, Plaintiffs fail to allege any harm derived from that conduct.

C. Clearview's Voluntary Changes

As Plaintiffs admit, earlier this year Clearview changed its business practices. Many of these measures were implemented "to avoid capturing faceprints of Illinois residents." Compl.

¶ 48. For example, Clearview no longer runs facial vectors on images from websites identified as being in Illinois, and Clearview has adjusted its collection methods to avoid running facial vectors on images with metadata associated with Illinois. *Id.* ¶¶ 48-50. Clearview also cancelled all contracts with Illinois entities, including all police departments in Illinois. Ex. A ¶ 16.

Clearview also cancelled all contracts with non-government entities anywhere in the world. *Id.* Clearview's current operations are thus exempt from BIPA, which provides that "[n]othing in this Act shall be construed to apply to a contractor, subcontractor, or agent of a State agency or local unit of government when working for that State agency or local unit of government." 740 ILCS 14/25(e). Because Plaintiffs seek only injunctive relief under BIPA, and because Clearview's current operations fall squarely within BIPA's government contractor exception, Plaintiffs' entire case is moot.[4]

D. Plaintiffs' BIPA Claim

Notwithstanding these changes, Plaintiffs filed their Complaint for injunctive relief based on alleged violations of BIPA. Compl. ¶¶ 66-74. Plaintiffs claim that Clearview's conduct violates Section 15(b) of BIPA, which provides that a private entity may not "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information" unless it (1) informs the person of the collection "in writing," (2) informs the person "in writing of the specific purpose and length of term" of the collection and storage, and (3) obtains a "written release" from the person. *Id.* ¶ 67; 740 ILCS 14/15(b). Plaintiffs also claim that Clearview's conduct violates Section 15(a), which requires a company in possession of

[4] Clearview is not moving to dismiss on this ground because Plaintiffs allege that Clearview has contracts with private entities. *See, e.g.*, Compl. ¶ 8. However, Plaintiffs' allegations are not accurate as applied to Clearview's current operations, and if the Complaint survives this motion to dismiss, Clearview anticipates filing a summary judgment motion based on the government contractor exception.

biometric data to provide a retention schedule or guidelines for destroying biometric data.[5]

ARGUMENT

This case should be dismissed for multiple reasons: (1) Clearview is not subject to personal jurisdiction in Illinois; (2) Plaintiffs' proposed application of BIPA is precluded by Illinois's extraterritoriality doctrine and the dormant Commerce Clause; (3) Plaintiffs' BIPA claim violates the First Amendment; and (4) BIPA does not apply to Clearview's technology.

II. Clearview Is Not Subject to Jurisdiction in Illinois.

Clearview is subject to jurisdiction in Illinois only if Plaintiffs establish that Clearview could be served under the Illinois long-arm statute. *See Morris v. Halsey Enters. Co.*, 379 Ill. App. 3d 574, 579 (1st Dist. 2008). And to satisfy the long-arm statute, Plaintiffs must demonstrate that Clearview's contacts with Illinois are sufficient to satisfy both federal and state due process concerns. *Id*. Because Plaintiffs cannot establish general or specific jurisdiction over Clearview, the Complaint should be dismissed.[6]

Specific jurisdiction exists when the defendant purposefully directs its activities at the forum state *and* the alleged injury arises out of those activities. *Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 472 (1985). Put another way, "even if a nonresident defendant purposefully directs its activities at a forum state, the cause of action must arise out of, or relate to, the defendant's contacts with the forum state." *Zamora v. Lewis*, 2019 IL App (1st) 181642, ¶ 47, *appeal denied*, 437 Ill. Dec. 586 (2020). In the context of online companies, courts "should be careful in resolving

[5] Contrary to Plaintiffs' allegation, Clearview posts its retention policy on its public website: https://clearview.ai/privacy/bipa. The Court may take judicial notice of Clearview's website. *CitiMortgage, Inc. v. Morales*, 2017 IL App (1st) 160657-U ¶ 33 n.2.

[6] Plaintiffs do not allege that Clearview is subject to general jurisdiction. To establish general jurisdiction, a plaintiff must show that a corporate entity is "at home" in Illinois, which Clearview, a Delaware company with headquarters in New York, is not. *Daimler AG v. Bauman*, 571 U.S. 117, 137 (2014).

questions about personal jurisdiction involving online contacts to ensure that a defendant is not haled into court simply because the defendant owns or operates an interactive website that is accessible in the forum state." *Matlin v. Spin Master Corp*, 921 F. 3d 701, 706 (7th Cir. 2019) (internal alterations omitted).

Plaintiffs here do not allege that Clearview took any actions in Illinois that gave rise to any alleged harm. Nor could they. Plaintiffs allege that Clearview marketed to or contracted with a number of Illinois companies, but they allege no other conduct on Clearview's part that was linked to the alleged harm to Plaintiffs. In fact, Plaintiffs do not even make an effort to demonstrate that Clearview's alleged actions in Illinois (*i.e.*, contracting with in-forum companies) are in any way associated with the harm allegedly suffered by Plaintiffs' members (*i.e.*, the alleged collection of their biometrics without prior consent). For that reason alone, there is no basis upon which to assert jurisdiction over Clearview because "a defendant's general connections with the forum are not enough" to establish specific jurisdiction, *Bristol-Myers Squibb Co. v. Superior Ct. of California.*, 137 S. Ct. 1773, 1781 (2017), as it is a "defendant's *suit-related* conduct [that] must create a substantial connection with the forum State." *Walden v. Fiore*, 571 U.S. 277, 284 (2014) (emphasis added). In analyzing a defendant's contacts with the forum state, courts may look only at the "very activity" out of which the "cause of action arises." *Keeton v. Hustler Magazine, Inc.*, 465 U.S. 770, 780 (1984). As the Seventh Circuit has recently emphasized, in doing that analysis, courts "consider the elements of the underlying tort for the light that they cast on 'the relationship between the defendant, the forum, and the litigation.' In that inquiry, [the] core focus is always on the defendants' conduct, not the plaintiffs' damages." *J.S.T. Corp. v. Foxconn Interconnect Tech. Ltd.*, 965 F.3d 571, 578 (7th Cir. 2020) (quoting *Walden*, 134 S. Ct. at 1121).

Plaintiffs' arguments in support of jurisdiction are each flawed as a matter of law. *First*,

Plaintiffs do not even allege that any of Clearview's conduct in Illinois gave rise to the BIPA violations alleged in the Complaint. Rather, Plaintiffs allege that Clearview "specifically marketed its service in Illinois." Compl. ¶ 62. Not only is this allegation belied by Plaintiffs' own allegations, it is insufficient because there is no alleged link between the services allegedly marketed in Illinois and any alleged harm to Plaintiffs. As Plaintiffs acknowledge, Clearview marketed its product nationally and internationally, which defeats the allegation that Clearview "targeted" Illinois. *See, e.g.*, *id.* ¶ 59 (alleging that Clearview "aggressively pursu[ed] clients" in "Europe, South America, Asia Pacific, and the Middle East"). As such, Illinois was not the "focal point" of any marketing efforts, as would be required to create jurisdiction. *See, e.g.*, *Calder* v. *Jones*, 465 U.S. 783, 789 (1984) (finding jurisdiction over defendant accused of libel for story published in California only because "California is the focal point both of the story and of the harm suffered"). Even where an out-of-state company "heavily advertised" in Illinois, specific jurisdiction has been found to be lacking when, as here, the claims do not arise from the activities in Illinois. *Zamora*, 2019 IL App (1st) 181642, ¶ 69.

For example, in *Gullen v. Facebook.com, Inc.*, Facebook (unlike Clearview) was "registered to do business" and had a "sales and advertising office" in Illinois, but even there the court rejected specific jurisdiction because these "contacts have no relationship to this suit, which arises from Facebook's alleged collection of biometric data from a photo, not from its sales, marketing, or other business activity in Illinois." No. 15 C 7681, 2016 U.S. Dist. LEXIS 6958, at *5 (N.D. Ill. Jan. 21, 2016). The same is true here. Likewise, in *Bray v. Lathem Time Co*., the court held that there was no specific jurisdiction over the non-resident defendant because "[t]his lawsuit concerns [defendant]'s alleged collection, storage, use and disclosure of biometrics—not [defendant]'s sales" and marketing. No. 19-3157, 2020 U.S. Dist. LEXIS 53419, at *10 (C.D. Ill.

Mar. 27, 2020). Similarly, here, even if Clearview did target Illinois for marketing purposes, that still would not confer specific jurisdiction because the alleged harm does not relate to Clearview's business in Illinois and in analyzing a defendant's contacts with the forum state, courts may look only at the "very activity" out of which the "cause of action arises." *Keeton*, 465 U.S. at 780.

Second, Plaintiffs allege in a conclusory manner that Clearview "has committed tortious acts expressly aimed at Illinois residents." Compl. ¶ 17. Again, Plaintiffs contradict their own allegations. Rather than "expressly aim[ing]" anything at Illinois residents, Plaintiffs allege that Clearview "has captured more than three billion faceprints" from across the globe. *Id.* ¶ 6. And for jurisdiction to lie, Illinois must be the "focal point" of Clearview's conduct, which Plaintiffs do not even allege is the case here. *Calder*, 465 U.S. at 789.

Not surprisingly, then, the *Gullen* court dismissed a complaint against Facebook for lack of personal jurisdiction in circumstances similar to those present here. 2016 U.S. Dist. LEXIS 6958. The *Gullen* plaintiff alleged that Facebook "target[ed]" Illinois residents with its facial-recognition technology, but the court rejected that allegation because the plaintiff elsewhere alleged that "Facebook uses facial recognition technology on every user-uploaded photo, not just on photos uploaded in or by residents of Illinois." *Id.* at *5. The *Gullen* court continued: "Because plaintiff does not allege that Facebook targets its alleged biometric collection activities at Illinois residents, the fact that its site is accessible to Illinois residents does not confer specific jurisdiction over Facebook." *Id.* at *7. Plaintiffs' allegations here fail for the same reasons.

Third, Plaintiffs allege that Clearview conducts business in Illinois by "actually selling its services to customers in Illinois." Compl. ¶¶ 17, 59. However, contracting with a forum-based entity alone does not create jurisdiction. *Burger King*, 471 U.S. at 478 ("If the question is whether an individual's contract with an out-of-state party *alone* can automatically establish sufficient

minimum contacts in the other party's home forum, we believe the answer clearly is that it cannot."). Moreover, "where a corporation is merely transacting business within the state, the state only has jurisdiction over those causes of action that arise out of the business transaction or transactions that took place within the state." *Old Orchard Urban Ltd. P'ship v. Harry Rosen, Inc.*, 389 Ill. App. 3d 58, 65 (1st Dist. 2009). Plaintiffs have not alleged any harm arising from Clearview's alleged contracts with Illinois entities. Rather, the harm purportedly suffered by Plaintiffs relates to Clearview's alleged collection of biometric information from Illinois residents. Plaintiffs do not—and cannot—allege that that conduct occurred in Illinois.

Clearview expects that Plaintiffs will point to Judge Coleman's decision in the Northern District of Illinois, which denied Clearview's motion to dismiss for lack of personal jurisdiction in a federal case alleging violations of BIPA. *Mutnick v. Clearview AI, Inc.,* No. 20-512, 2020 U.S. Dist. LEXIS 144583 (N.D. Ill. Aug. 12, 2020). Clearview respectfully submits that Judge Coleman's decision was wrongly decided. For one thing, Judge Coleman accepted the plaintiffs' conclusory allegation that Clearview "directed [its] 'illegal harvesting' operation at the State of Illinois," even though this was contradicted by the plaintiffs' own complaint and Clearview's uncontested declaration. *Id.* at *6. Likewise, Judge Coleman found that Clearview's agreements with Illinois law enforcement agencies show that Clearview "sold, disclosed, obtained, and profited from the biometric identifiers of Illinois citizens." *Id.* Again, this contradicted a declaration submitted by Clearview's president. Judge Coleman also did not address the legal authorities cited by Clearview, including those detailed above. For all of these reasons, Clearview is not subject to personal jurisdiction in Illinois.

III. BIPA Does Not Regulate Out-Of-State Conduct

The Complaint also fails because (1) BIPA does not apply to conduct outside of Illinois

and (2) any such application of BIPA would violate the dormant Commerce Clause.

A. The BIPA Claim Violates the Extraterritoriality Doctrine

Illinois has a "long-standing rule of construction" that a "statute is without extraterritorial effect unless a clear intent in this respect appears from the express provisions of the statute." *Avery v. State Farm Mut. Auto. Ins. Co.*, 216 Ill. 2d 100, 184-85 (2005). Because BIPA expresses no such intent, courts in Illinois have repeatedly held that BIPA does not regulate out-of-state conduct. *See, e.g.*, *Rivera v. Google, Inc.*, 238 F. Supp. 3d 1088, 1104 (N.D. Ill. 2017) ("[BIPA] was not intended to and does not have extraterritorial application."); *Monroy v. Shutterfly, Inc.*, No. 16 C 10984, 2017 U.S. Dist. LEXIS 149604, at *15 (N.D. Ill. Sept. 15, 2017) (same). Accordingly, to state a BIPA claim, Plaintiffs must allege that the asserted violations occurred in Illinois. *See Rivera*, 238 F. Supp. 3d at 1100.

The Illinois Supreme Court has explained that a "transaction may be said to take place within a state if the circumstances relating to the transaction occur[red] *primarily and substantially*" in Illinois. *Avery*, 216 Ill. 2d at 186 (emphasis added). To satisfy this standard, the "*majority* of circumstances relating to the alleged violation" of the applicable statute must have occurred in Illinois. *Landau*, 381 Ill. App. 3d at 65 (emphasis added).

Illinois courts regularly grant motions to dismiss based on the extraterritoriality doctrine where, as here, the complaint fails to allege that the relevant facts occurred "primarily and substantially" in Illinois. *See, e.g.*, *Vulcan Golf, LLC v. Google Inc.*, 552 F. Supp. 2d 752, 775 (N.D. Ill. 2008) ("While the plaintiffs contend that Illinois has 'significant contacts' with each of the named class plaintiffs because each is a resident of the state and each conducts substantial business in this state, the plaintiffs point to no allegations that plausibly suggest that the purported deceptive domain scheme occurred primarily and substantially in Illinois."); *Landau*, 381 Ill. App.

3d at 63-65 (dismissing complaint because the harmful conduct occurred in Pennsylvania); *Stroman Realty, Inc. v. Allison*, 2017 IL App (4th) 150501-U, ¶ 61 (dismissing complaint where the defendant "solicit[ed] and advertis[ed] in Illinois" "remotely from Texas"); *Phillips v. Bally Total Fitness Holding Corp.*, 372 Ill. App. 3d 53, 58-59 (1st Dist. 2007); *Hackett v. BMW of N. Am., LLC*, No. 10 C 7731, 2011 U.S. Dist. LEXIS 71063, at *5-6 (N.D. Ill. June 30, 2011).

Plaintiffs' BIPA claim fails because Plaintiffs do not allege that any significant circumstances—let alone the "majority of circumstances"—occurred in Illinois. The BIPA claim boils down to this allegation: "[u]sing face recognition technology, Clearview has captured more than three billion faceprints from images available online, all without the knowledge—much less the consent—of those pictured." Compl. ¶ 6. However, Plaintiffs do not allege that Clearview "captured" these publicly-available images from Illinois (nor could they); Plaintiffs do not allege that Clearview scanned any images to create "faceprints" in Illinois (nor could they); and Plaintiffs do not allege that Clearview's "database" is located on servers in Illinois (nor could they). In fact, Plaintiffs do not allege that Clearview has ever had any contact with any of their members. Accordingly, Plaintiffs' BIPA claim should be dismissed because the "circumstances relating to the alleged violation" of BIPA—*i.e.*, the alleged "capturing, storing, and using" of biometric information, *id.* ¶ 73—did not occur in Illinois at all. *Landau*, 381 Ill. App. 3d at 65.

The residency of Plaintiffs' members does not change this conclusion. The location of the alleged violation is the most important consideration in the extraterritoriality analysis. *See, e.g.*, *Avery*, 216 Ill. 2d at 182, 186 (the extraterritoriality analysis is not "based on the residency of the plaintiff," but on whether "the circumstances relating to the transaction occur primarily and substantially within" Illinois); *Vulcan Golf*, 552 F. Supp. 2d at 775 (same); *Valley Air Serv. v. Southaire, Inc.*, No. 06 C 782, 2009 U.S. Dist. LEXIS 32709 at *36-37 (N.D. Ill. Apr. 16, 2009).

In their opposition, Plaintiffs may rely on several distinguishable cases from the Northern District of Illinois in which courts held that it was premature to grant a motion to dismiss a BIPA claim based on the extraterritoriality doctrine. In two cases, the plaintiffs uploaded photos of themselves to the defendants' product from a computer or device located in Illinois. *See, e.g.*, *Rivera*, 238 F. Supp. 3d at 1101 ("[Plaintiff's] photographs were allegedly 'automatically uploaded in Illinois to [defendant's] cloud-based Google Photos service . . . from an Illinois-based Internet Protocol ('IP') address"); *Monroy*, 2017 U.S. Dist. LEXIS 149604, at *15-16 ("[T]he complaint alleges that the photo of Monroy was uploaded to Shutterfly's website from a device that was physically located in Illinois and had been assigned an Illinois-based IP address").[7] Thus, the defendants directly interacted with the plaintiffs and engaged in relevant conduct in Illinois. By contrast, Plaintiffs here do not allege that they have ever interacted with Clearview, let alone in Illinois. In a third case, the defendant had a "regional headquarters in Chicago, Illinois." *Vance v. IBM Corp.*, No. 20-cv-577 (N.D. Ill. Mar. 12, 2020), ECF No. 19 ¶ 13.

B. Plaintiffs' Application of BIPA Would Violate the Dormant Commerce Clause

If BIPA were to apply to Clearview, then BIPA would violate the U.S. Constitution. Under Article I, Section 8, Congress has the exclusive power to regulate commerce "among the several States." This express grant of power limits the "authority of the States to enact legislation affecting interstate commerce." *Healy v. Beer Inst., Inc.,* 491 U.S. 324, 326 n.1 (1989). The "dormant Commerce Clause" "precludes the application of a state statute" that has "the practical effect of . . . control[ling] conduct beyond the boundaries of the State," "whether or not the commerce has effects within the State." *Id.* at 336. Thus, the dormant Commerce Clause "protects against

[7] Likewise, in *Patel v. Facebook, Inc.*, the plaintiffs were Illinois users of Facebook who had uploaded their photos to Facebook from Illinois. 932 F.3d 1264, 1268 (9th Cir. 2019).

inconsistent legislation arising from the projection of one state regulatory regime into the jurisdiction of another State." *Id.* at 337. Absent this rule, "any state that has chosen a policy more laissez faire than [another state's] would have its choices stymied, because the state that has chosen more regulation could always trump its deregulated neighbor." *Morley-Murphy Co. v. Zenith Elecs. Corp.,* 142 F.3d 373, 379 (7th Cir. 1998). Illinois courts have "t[aken] a broad[] view" of what constitutes an inconsistent legal regime for purposes of the dormant Commerce Clause analysis. *Midwest Title Loans, Inc. v. Mills*, 593 F.3d 660, 667-68 (7th Cir. 2010). Specifically, a party need not show "inconsistent *obligations*"; rather, "the *absence* of a . . . counterpart" law in another state shows that the other state "thinks [the conduct] shouldn't be restricted in the [same] way." *Id.* at 667 (emphasis added).

Here, New York has recently considered BIPA-style legislation four times, but each time the proposed bill failed to pass. *See* A1911, Assemb., Reg. Sess. (N.Y. 2019); S1203, Senate, Reg. Sess. (N.Y. 2019); A9793, Assemb., Reg. Sess. (N.Y. 2018); S8547, Senate, Reg. Sess. (N.Y. 2018). Because Illinois has no interest in regulating Clearview's alleged conduct in New York, and because New York has declined to adopt a statute regulating biometrics, the dormant Commerce Clause precludes Plaintiffs' proposed application of BIPA, which would "exalt the public policy" of Illinois over that of New York. *Midwest*, 593 F.3d at 668.[8]

Applying BIPA to Clearview's conduct in New York would subject Clearview to liability under an Illinois statute merely because some small percentage of Clearview's alleged database of

[8] This principle is especially important in the Internet context. "[C]ourts have long recognized that certain types of commerce demand consistent treatment," and that the "Internet represents one of those areas." *Am. Libraries Ass'n v. Pataki*, 969 F. Supp. 160, 181 (S.D.N.Y. 1997) ("Regulation by any single state can only result in chaos, because at least some states will likely enact laws subjecting Internet users to conflicting obligations."); *see also Am. Booksellers Found. v. Dean,* 342 F.3d 96, 103 (2d Cir. 2003) ("Because the internet does not recognize geographic boundaries, it is difficult . . . for a state to regulate internet activities without project[ing] its legislation into other States.").

"three billion" publicly-available photographs contain images of Illinois residents. Compl. ¶ 6. Moreover, Plaintiffs admit that it is impossible to determine whether many publicly-available photographs have any connection to Illinois. *See id.* ¶ 48 ("[A] significant proportion of photos of Illinois residents that appear online will not contain geolocation information."); *id.* ¶ 49 ("IP address geolocation databases are notoriously unreliable for determining a user's location."). Because in many instances it is in fact impossible to identify where a photo on the Internet comes from—or where the person in the photo resides—under Plaintiffs' application of BIPA, Clearview arguably could not collect those photographs on the Internet simply because they might relate in some way to someone in Illinois. This is precisely the kind of burden on interstate commerce that the dormant Commerce Clause prohibits.

Plaintiffs will likely rely on cases holding that the dormant Commerce Clause argument is premature at the motion to dismiss stage, but those cases are distinguishable. In *Monroy*, for example, the court emphasized that the plaintiff's "suit, as well as his proposed class, is confined to individuals whose biometric data was obtained from photographs *uploaded to Shutterfly in Illinois*." 2017 U.S. Dist. LEXIS 149604, at *20 (emphasis added). The court concluded that "[a]pplying BIPA in this case would not entail any regulation of Shutterfly's gathering and storage of biometric data *obtained outside of Illinois*"; rather, "the statute requires Shutterfly to comply with certain regulations if it wishes to *operate in Illinois*." *Id.* (emphasis added). By contrast, Plaintiffs' BIPA claim purports to regulate the collection of "biometric information obtained outside of Illinois." *Id.* Moreover, unlike in *Monroy*, Plaintiffs expressly allege that it is difficult, if not impossible, to determine whether many publicly-available photographs are taken in Illinois or are of Illinois residents. Compl. ¶¶ 48-50. Accordingly, the face of the Complaint here confirms that Plaintiffs' allegations cover biometric data obtained outside Illinois and thus violate the U.S.

Constitution because Plaintiffs' requested injunctive relief would inevitably impact Clearview's conduct in many other states.[9]

IV. Plaintiffs' Claim Is Barred by the First Amendment and Article One Section Four of the Illinois Constitution

Plaintiffs' claim relies solely on BIPA, which, among other things, prohibits entities from collecting or otherwise obtaining a person's biometric identifiers without informing that person that it will be doing so and obtaining her advance, written consent. What Plaintiffs do not even refer to, however, is the First Amendment to the U.S. Constitution, notwithstanding that its application to this case requires dismissal of Plaintiffs' claim. For the same reasons that BIPA violates the First Amendment as set forth below, BIPA also violates the free speech protections of the Illinois Constitution, which provides "greater protection to free speech than does its Federal counterpart." *People v. DiGuida*, 152 Ill. 2d 104, 121 (1992); *see also* Ill. Const. 1970, art. I, § 4.

A. Clearview Is Engaged in Speech That Is Protected by the First Amendment

Clearview's creation and use of its app constitute protected speech under the First Amendment. *First*, Clearview's collection and use of publicly-available photographs are protected under the First Amendment. The "creation and dissemination of information are speech within the meaning of the First Amendment." *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 570 (2011); *accord People v. Austin*, 2019 IL 123910, ¶ 31. BIPA's restrictions on the collection of "biometric information" in publicly-available photographs violate the First Amendment because they inhibit Clearview's ability to use this public information in Clearview's search engine.

[9] In *Vance v. IBM*, the court concluded that it did not have enough information at the pleading stage "to know the extent to which IBM's actions occurred in Illinois and whether the Dormant Commerce Clause bars this suit." 20 C 577, 2020 U.S. Dist. LEXIS 168610, at *10 (N.D. Ill. Sept. 15, 2020). For the reasons described above, the Court does not lack that information here.

Second, because Clearview's service is a search engine, it is protected speech under the First Amendment. *Cf. Austin*, 2019 IL 123910, ¶ 31 ("[F]irst [A]mendment protections for speech extend fully to Internet communications.") (citation omitted).[10] Courts have repeatedly held that the activities of search engines constitute speech entitled to First Amendment protection because they require the types of judgments about what to publish that trigger free speech considerations. *See, e.g.*, *Search King, Inc. v. Google Tech., Inc.*, No. CIV-02-1457-M, 2003 U.S. Dist. LEXIS 27193, at *11-12 (W.D. Okla. May 27, 2003) (Google's rankings of search results were "subjective result[s]" that amounted to "constitutionally protected opinions" "entitled to full constitutional protection"). Clearview's app makes similar judgments about what information will be most useful to its users, who seek publicly-available photos and information that help identify individuals in photos that the users upload to the app.

Central to this case is the indisputable proposition that all information of potential relevance to this case is and has been publicly available. As the Complaint acknowledges, all challenged acts of Clearview relate to "photographs available online" on Facebook and other websites. Compl. ¶ 44, 45. Although the dissemination of photographs portraying private sexual conduct may well not be protected by the First Amendment, *Austin*, 2019 IL 123910, ¶ 119,[11] the republication of voluntarily posted photographs on the Internet is. Once "truthful information is

[10] In *Zhang v. Baidu.com, Inc.*, the court recognized that "there is a strong argument to be made that the First Amendment fully immunizes search-engine results from most, if not all, kinds of civil liability and government regulation" and explained that "[t]he central purpose of a search engine is to retrieve relevant information from the vast universe of data on the Internet and to organize it in a way that would be most helpful to the searcher. In doing so, search engines inevitably make editorial judgments about what information (or kinds of information) to include in the results and how and where to display that information." 10 F. Supp. 3d 433, 438 (S.D.N.Y. 2014).

[11] It is noteworthy that Plaintiff ACLU has repeatedly opposed on First Amendment grounds the adoption of legislation drafted to protect the victims of nonconsensual pornography—revenge porn—however egregious the loss of their privacy. *See* Elena Lentz, *Revenge Porn and the ACLU's Inconsistent Approach*, 8 Ind. J.L. & Soc. Equality 155 (2020).

publicly revealed or in the public domain, a court may not constitutionally restrain its dissemination." *In re Minor*, 205 Ill. App. 3d 480, 491 (4th Dist. 1990), *aff'd*, 149 Ill. 2d 247 (1992).

A recent Seventh Circuit case is similarly illustrative of the proposition. In *Nieman v. VersusLaw, Inc.*, 512 F. App'x 635 (7th Cir. 2013), the plaintiff sued Yahoo!, Google, Microsoft, and VersusLaw, alleging that search engines operated by these companies enabled potential employers to find documents related to a lawsuit he had brought against a past employer, which allegedly caused the potential employers not to hire him due to his perceived litigiousness. *Id.* at 636. The Seventh Circuit affirmed dismissal on First Amendment grounds, holding that plaintiff's claims were barred because they were "based on the defendants' republication of documents contained in the public record, so they fall within and are barred by the First Amendment privilege." *Id*. at 638. A similar First Amendment privilege protects Clearview's republication of publicly-available photos openly published on the Internet.

In fact, courts have repeatedly held that individuals have no right to privacy in materials they post on the Internet. *See United States v. Khan*, No. 15-cr-286, 2017 U.S. Dist. LEXIS 82493, at *19-*20 (N.D. Ill. May 31, 2017) (holding that "[t]here is no expectation of privacy in a public Facebook page" because "[a]lthough a person generally has a reasonable expectation of privacy in the contents of his own personal computer . . . such an expectation may be extinguished 'when a computer user disseminates information to the public through a website'") (citations omitted), *aff'd*, 937 F.3d 1042 (7th Cir. 2019).[12] As the Plaintiffs make unambiguously clear, the

[12] *See also Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001) ("Users [of the Internet] would logically lack a legitimate expectation of privacy in the materials intended for publication or public posting."); *Doe v. Yesner*, No. 3:19-cv-0136-HRH, 2019 U.S. Dist. LEXIS 150133 (D. Alaska Sept. 4, 2019) (holding that the use of photographs posted on plaintiff's social media profile could not support claims for intrusion of solitude or public disclosure of private facts); *Nucci v. Target Corp.*, 162 So. 3d 146, 153 (Fla. Dist. Ct.

photographs in Clearview's database are publicly available, Compl. ¶ 54, and were voluntarily placed in the public sphere by Plaintiffs' members, clients, and program participants, *id.* ¶ 45 ("Plaintiffs' members, clients, and program participants, like millions of other Illinois residents, have uploaded numerous photos of themselves to social media sites and other websites.").

B. BIPA Is a Content-Based Restriction Subject to First Amendment Scrutiny and Presumptively Unconstitutional

BIPA is a content-based statute because it "target[s] speech based on its communicative content." *Reed v. Town of Gilbert*, 576 U.S. 155, 163 (2015). Content-based regulations "are presumptively unconstitutional and may be justified only if the government proves that they are narrowly tailored to serve compelling state interests." *Nat'l Inst. of Family & Life Advocates v. Becerra*, 138 S. Ct. 2361, 2371 (2018) (citing *Reed*, 576 U.S. at 163) ("*NIFLA*"); *accord People v. Relerford*, 2017 IL 121094, ¶ 32. In this case, Plaintiffs have never maintained that Clearview could be barred or limited from seeking to match photographs that appeared on Facebook or other websites with those uploaded by licensed users of Clearview's service if the matching were done in a particularly cumbersome way—for example, by hiring a vast team of researchers to review and match photos manually. Their objection is seeking to do functionally the same act by the use of modern technology. BIPA does this by targeting specific content—defined as "Biometric Information" and "Biometric Identifiers," 740 ILCS 14/10,—and not others (*e.g.*, photographs), simply because that content allows for an efficient means of identifying individuals. That makes the statute content-based and, under *Reed* and *NIFLA*, triggers strict scrutiny.

BIPA restricts, in the name of privacy, Clearview's ability to "collect, capture, purchase, receive through trade, or otherwise obtain," or "profit from" the publicly-available information

App. 2015) ("We agree with those cases concluding that, generally, the photographs posted on a social networking site are neither privileged nor protected by any right of privacy, regardless of any privacy settings.").

Clearview uses in its search engine. 740 ILCS 14/15(b), (c). However, the Supreme Court recognized in *Sorrell* that, because "[f]acts . . . are the beginning point for much of the speech that is most essential to advance human knowledge," laws that burden the underlying inputs of speech implicate the First Amendment. 564 U.S. at 570.

In *Sorrell*, the Court held that the statute at issue violated the First Amendment, in part, because its "purpose and practical effect" was to, in the name of privacy, "diminish the effectiveness of marketing by manufacturers of brand-name drugs." *Id.* at 565. Under the statute, pharmacies were prohibited from selling information about doctors' prescribing habits to third-parties, including so-called "data miners" who would produce reports and lease them to pharmaceutical manufacturers. *Id.* at 558. However, the statute did not prohibit pharmaceutical manufacturers from more cumbersome methods of learning this information, including by calling individual doctors and asking them about their prescribing habits. Like the statute in *Sorrell*, the "purpose and practical effect" of BIPA on Clearview is to unconstitutionally limit Clearview's effectiveness in communicating with the users of its app information about the public photographs they upload.

The Court in *Sorrell* also referred back to its earlier ruling in *United States v. O'Brien*, 391 U.S. 367, 384 (1968), and stated that "the inevitable effect of a statute on its face may render it unconstitutional." *Sorrell*, 564 U.S. at 565. Here, BIPA's inevitable effect would be nothing less than preventing the identification of individuals whose published photographs were on the Internet. The First Amendment does not permit a state to accomplish this goal. Plaintiffs' Complaint makes plain that it is the efficiency of Clearview's app—made possible by the use of facial vectors—that allegedly triggers the privacy concerns that BIPA is designed to protect. *See, e.g.*, Compl. ¶ 3 (alleging that the capture of "faceprints" can "lead to unwanted tracking and invasive surveillance

by making it possible to *instantaneously* identify everyone at a protest or political rally, a house of worship . . . and more") (emphasis added); *id.* ¶ 6 ("[Clearview] can *instantaneously* identify the subject of a photograph with unprecedented accuracy, enabling covert and remote surveillance of Americans on a massive scale.") (emphasis added). But the First Amendment prohibits the application of laws that have the purpose and/or practical effect of burdening speech by reducing the effectiveness of its content. *See Sorrell*, 564 U.S. at 565 (striking down law as content-based, in part, because its "purpose and practical effect are to diminish the effectiveness of marketing by manufacturers of brand-name drugs"); *R.A.V. v. City of St. Paul*, 505 U.S. 377, 386 (1992) (noting that the government may not regulate the use of sound trucks, a tool for amplifying speech, "based on hostility—or favoritism—towards the underlying message expressed").

C. As Applied to Clearview, BIPA Is Subject to and Cannot Survive Strict Scrutiny

Because BIPA imposes content-based restrictions on Clearview's speech, it is subject to strict scrutiny. That demanding standard cannot be met unless "the restriction furthers a compelling interest and is narrowly tailored to achieve that interest." *Reed*, 576 U.S. at 171 (internal quotation marks and citation omitted). BIPA fails this test.

First, BIPA does not serve any compelling state interest with respect to already-published public information. The stated purpose of BIPA is to protect the privacy of Illinois citizens. *See, e.g.*, *Bryant v. Compass Grp. USA, Inc*., 958 F.3d 617, 619 (7th Cir. 2020) (finding that BIPA's "regime is designed to protect consumers against the threat of irreparable privacy harms"). Specifically, BIPA purports to protect material that is "confidential and sensitive." 740 ILCS 14/15(e)(2). But as in this case, any information that an individual makes available to the general public is by definition not "confidential" or "sensitive." *Cf. Bernal v. ADP, LLC*, No. 2017-CH-12364, 2019 Ill. Cir. LEXIS 1025, at *3 n.9 (Cir. Ct. Cook Cty. Aug. 23, 2019) (recognizing that

BIPA does not apply if plaintiffs waive "the right to control their biometric information").

The Supreme Court "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979); *accord United States v. Caira*, 833 F.3d 803 (7th Cir. 2016); *see also* Restatement (Second) of Torts § 652D (1977) ("[T]here is no liability for giving further publicity to what the plaintiff himself leaves open to the public eye."). And as we have previously demonstrated, this is particularly well-established with respect to photographs posted on the Internet. Because these photographs are public (and, by definition, not "confidential" or "sensitive"), Plaintiffs' members have waived any right to privacy as to them, and therefore the state has no interest—let alone a compelling one—in protecting the "privacy" of information contained in or about these photographs.

Second, even if the state had a compelling interest in protecting the privacy of individuals who placed photographs of themselves in the public realm (and it does not), BIPA is not narrowly tailored to achieve that interest. As applied to Clearview, BIPA would require Clearview to provide written notice to the individuals whose photographs are in Clearview's database and obtain a "written release" before collecting their "biometric information." 740 ILCS 14/15(b). But the individuals who posted their photographs on the Internet effectively consented to sharing their "biometric information," which is embedded in their photographs, with the public at large. *See, e.g.*, *Caira*, 833 F.3d at 806 ("[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties[.]").

D. BIPA Is Unconstitutionally Overbroad

Even if strict scrutiny were not applied in this case, the statute would be unconstitutionally overbroad and should, at the least, be narrowed to protect the publicly-disclosed data that

Clearview provides. A statute "lacks the precision that the First Amendment requires when a statute . . . effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another." *Reno v. ACLU*, 521 U.S. 844, 874 (1997); *see also People v. Sequoia Books, Inc*., 127 Ill. 2d 271, 288 (1989) (recognizing that "regulation of any form of expression, even of obscenity, [must] be carefully drawn so as not to impact unduly upon protected speech"); *Austin*, 2019 IL 123910, ¶ 89 (recognizing that a First Amendment challenge based on "overbreadth is permitted out of concern that the threat of enforcement of an overbroad law may chill or deter constitutionally protected speech").

Here, as explained above, because of the limited ability to discern where subjects of online photographs may reside, BIPA all but bars—and certainly burdens—Clearview's right to use previously-published publicly-displayed photographs in a manner that enables Clearview to match those photographs with other photographs in the possession of Clearview's users. In doing so, BIPA "suppresses a large amount of speech" that is fully protected under the First Amendment, precisely what the overbreadth doctrine exists to protect against. *Reno*, 521 U.S. at 874; *see also United States v. Stevens*, 559 U.S. 460, 473 (2010) ("[A] law may be invalidated as overbroad if 'a substantial number of its applications are unconstitutional, judged in relation to the statute's plainly legitimate sweep.'") (citation omitted).

BIPA is not narrowly drafted because it would require Clearview to obtain written consent from individuals whose names are unknown to it and who have already consented to the general public viewing their photos. The practical effect of this overly-broad drafting would be to require Clearview to abandon its constitutionally-protected business activities. Such a requirement cannot withstand strict scrutiny and is thus unconstitutional.

V. BIPA Does Not Apply to Clearview's Use of Photographs

Plaintiffs' BIPA claim fails for yet another independent reason: the plain language of BIPA expressly excludes both photographs and information derived from photographs.

BIPA covers two categories of information: (1) original sources of information about a person ("biometric identifiers," defined as a "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry") and (2) data derived from those sources ("biometric information," defined as "information . . . based on an individual's biometric identifier"). 740 ILCS 14/10. BIPA's definition of "biometric identifiers" excludes "photographs," and its definition of "biometric information" excludes "information derived from items or procedures excluded under the definition of biometric identifiers," such as photographs. *Id.* Accordingly, the legislature excluded both photographs and information derived from photographs from BIPA's reach.

Plaintiffs nonetheless argue that Clearview's collection of biometric data "from photographs available online" violates BIPA because Clearview's "[f]aceprints are scans of facial geometry." Compl. ¶¶ 31, 44. In addition to ignoring BIPA's clear photograph exclusion, the collection of biometric data from photographs plainly falls outside of what the legislature intended, since the statute was clearly intended to cover biometric information collected personally from an individual. Each of BIPA's covered biometric identifiers describes an in-person process for obtaining information about an individual.[13] The statute was not intended to encompass biometrics

[13] For example, a "retina scan" refers to a live person holding her eye to a scanner that casts a beam of low-energy infrared light into the eye (https://www.biometricupdate.com/201307/explainer-retinal-scan-technology); a "fingerprint" refers to a live person pressing her finger to the surface of either a card or scanning device (https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/recording-legible-fingerprints); a "voiceprint" refers to a live person's spoken word (https://www.sans.org/reading-room/whitepapers/authentication/exploration-voicebiometrics-1436); and a "scan of hand . . . geometry" refers to a person placing her live hand on a "plate, palm down, and guided by five pegs that sense when the hand is in place," and then a camera "captur[ing] a silhouette image of the hand" (https://www.biometricupdate.com/201206/explainer-hand-geometry-recognition).

not collected personally.[14] As further support for this interpretation, BIPA requires an entity to obtain "written consent" before it collects biometric data. 740 ILCS 14/15(b). If a facial scan is performed in person, this "written consent" requirement is at least possible. However, if BIPA includes biometric information derived from photographs on the public Internet, it would often be impossible to comply with this provision. The Court should not interpret BIPA in a way that renders it impossible to comply with its terms. *See Clinton v. City of New York*, 524 U.S. 417, 429 (1998) (rejecting statutory interpretation that "would produce an absurd and unjust result").

Accordingly, Clearview's use of photographs available on the public Internet is not covered by BIPA because the statute exempts photographs and any information derived from photographs.

The federal cases that have held that BIPA applies to scans of facial geometry derived from photographs are not persuasive. As an initial matter, Clearview is aware of no Illinois state court cases addressing this issue. As to the federal cases, the court in *Facebook* concluded that BIPA's use of the word "photographs" refers only to "paper prints of photographs," but there is no textual basis for that conclusion. *In re Facebook Biometric Info. Privacy Litig.*, 185 F. Supp. 3d 1155, 1171 (N.D. Cal. 2016). Other courts have likewise failed to give proper weight to BIPA's clear textual exclusion of "photographs" from the meaning of biometric identifiers and "information derived from" photographs. *Vance*, 2020 U.S. Dist. LEXIS 168610, at *10-12; *Monroy*, 2017 U.S. Dist. LEXIS 149604, at *5-14; *Rivera*, 238 F. Supp. 3d 1088.

CONCLUSION

For all these reasons, Clearview respectfully requests that the Court dismiss the Complaint.

[14] BIPA's "Legislative findings" section confirms this reading. Specifically, the "Legislative Findings" detail the concerns that motivated BIPA's passage, which included the increasing use of "biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias"—all of which are in-person transactions. 740 ILCS 14/5.

DATED: October 7, 2020

JENNER & BLOCK LLP

By: *s/ David P. Saunders*

Lee Wolosky (pro hac vice pending)
Andrew J. Lichtman (pro hac vice forthcoming)
JENNER & BLOCK LLP
919 Third Avenue
New York, New York 10022-3908
Phone: (212) 891-1600
lwolosky@jenner.com
alichtman@jenner.com

David P. Saunders
Howard S. Suskin
JENNER & BLOCK LLP
353 North Clark Street
Chicago, Illinois 60654
Phone: (312) 222-9350
hsuskin@jenner.com
dsaunders@jenner.com

Floyd Abrams (pro hac vice pending)
Joel Kurtzberg (pro hac vice pending)
CAHILL GORDON & REINDEL LLP
32 Old Slip
New York, NY 10005
Phone: (212) 701-3000
fabrams@cahill.com
jkurtzberg@cahill.com

Attorneys for Defendant Clearview AI, Inc.

CERTIFICATE OF SERVICE

I, David Saunders, an attorney, hereby certify that I caused a copy of the foregoing Memorandum of Law to be served on all counsel of record via email on this 7th day of October 2020.

Jay Edelson
jedelson@edelson.com
Benjamin H. Richman
brichman@edelson.com
David I. Mindell
dmindell@edelson.com
J. Eli Wade-Scott
ewadescott@edelson.com
Edelson PC
350 North LaSalle Street, 14th Floor
Chicago, IL 60654
3120589-6370

Rebecca K. Glenberg
rglenberg@aclu-il.org
Karen Sheley
ksheley@aclu-il.org
Juan Caballero
jcaballero@aclu-il.org
Roger Baldwin Foundation of ACLU, Inc.
180 North Michigan Avenue, Suite 2300
Chicago, Illinois 60601
Tel: 312.201.9740

Nathan Freed Wessler
nwessler@aclu.org
Vera Eidelman
veidelman@aclu.org
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
212-549-2500

By: /s/ *David P. Saunders*
David P. Saunders