IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION OF ILLINOIS, CHICAGO ALLIANCE AGAINST SEXUAL EXPLOITATION, SEX WORKERS OUTREACH PROJECT CHICAGO, ILLINOIS STATE PUBLIC INTEREST RESEARCH GROUP, INC., and MUJERES LATINAS EN ACCIÓN, *Plaintiffs*, v. CLEARVIEW AI, INC., a Delaware corporation, *Defendant*.	Case No.: 2020 CH 04353 Calendar 11 Honorable Pamela McLean Meyerson

PLAINTIFFS' RESPONSE TO DEFENDANT'S MOTION TO DISMISS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

United States Supreme Court Cases

United States Appellate Court Cases

United States District Court Cases

Illinois Supreme Court Cases:

Illinois Appellate Court Cases:

Illinois Circuit Court Cases:

Statutory Provisions:

Other Authorities:

Surreptitiously, and without consent, Defendant Clearview AI, Inc. ("Clearview") captured the unique biometric identifiers of countless Illinoisans and used them to amass what it calls the "world's best facial recognition technology combined with the world's largest database of headshots." (Compl. ¶ 55.) Clearview relies on "faceprints," which are biometrics calculated using measurements between various features on an individual's face.

Because everyone's face is different, everyone's faceprint is unique—much like everyone's fingerprint or DNA profile. Unlike a social security or passport number, once compromised, a person cannot change their faceprint or protect it. Nonconsensual capture therefore presents a serious risk to security and enables intrusive tracking that invades privacy.

Illinois, fortunately, has taken steps to curb such abuses. Passed in 2008, the Biometric Information Privacy Act ("BIPA"), 740 ILCS 14, requires entities that wish to collect biometric identifiers like a faceprint from an individual to first provide notice, and obtain informed written consent, from that person. These protections, which our Supreme Court has noted are "particularly crucial in our digital world," *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, ¶ 34, ensure that Illinoisans retain control over their biometric identifiers.

Clearview violated BIPA, thereby violating the privacy and security of Illinoisans. Even though Clearview marketed its massive database to dozens of entities in Illinois—and even though the database undoubtedly contains the faceprints of millions of Illinoisans—Clearview failed to provide notice or obtain consent from any of the affected individuals. Plaintiffs are organizations whose members have been harmed by Clearview's nonconsensual capture of their faceprints. On behalf of their members, they seek retrospective and prospective injunctive relief.

Clearview's bid to dismiss Plaintiffs' lawsuit falls flat at every turn. First, Clearview contends that Illinois courts do not have jurisdiction over it. A federal court in Chicago recently

rejected this argument, and this Court should, too. Clearview is subject to this Court's jurisdiction because it collected the biometric identifiers of Illinoisans, and then used those Illinoisans' identifiers in a database it provided to Illinois entities.

Second, Clearview is incorrect that Plaintiffs' claim violates Illinois's rule against the extraterritorial application of its laws, or the dormant Commerce Clause. Illinois has the power to regulate what companies do with Illinoisans' biometric data. This requires no extraterritorial application of the law and interferes with no other states' regulation.

Third, applying BIPA to Clearview does not violate the First Amendment. BIPA's notice-and-consent requirement regulates conduct, not speech. To the extent that BIPA has an incidental effect on Clearview's speech, the law survives First Amendment scrutiny—including as applied to Clearview—because it advances the state's substantial interests in protecting Illinoisans' privacy and security, and it neither seeks to, nor in fact does, suppress expression.

Finally, Clearview asserts that BIPA does not prohibit the collection of faceprints from photographs. Every court to have considered this argument has rejected it, as it conflicts with BIPA's plain language, and with common sense. The motion to dismiss should be denied.

BACKGROUND

Pursuant to BIPA, entities must provide notice to and obtain individualized, informed, and written consent from individuals before capturing their biometric identifiers. 740 ILCS 14/15(b). BIPA defines a "biometric identifier" as a "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry" (*i.e.*, a unique algorithmic or mathematical representation of physical features allowing for personal identification). 740 ILCS 14/10. These protections are necessary because biometric identifiers are "biologically unique to the individual; therefore, once compromised, the individual has no recourse, [and] is at heightened risk for identity theft" and

other privacy harms. 740 ILCS 14/5(c).

In January 2020, the New York Times revealed that Clearview had used face recognition technology to surreptitiously capture more than three billion faceprints from images gathered from across the internet. Compl. ¶¶ 1, 6–7, 44. The faceprints captured by Clearview are scans of face geometry, and therefore are a "biometric identifier" subject to BIPA's protections. *Id.* ¶ 31. Yet Clearview captured these billions of faceprints, including those of countless Illinoisans, without providing notice to or obtaining consent from individuals. *Id.* ¶ 6. Clearview has sold or provided access to its faceprint database to thousands of public and private entities, including more than 105 corporations and government agencies in Illinois. *Id.* ¶¶ 8, 62. Those entities are able to use Clearview's system to instantaneously capture faceprints from a photograph, enabling covert and remote surveillance of Americans on a massive scale. *Id.* ¶ 6. And Clearview's mass faceprint database is vulnerable to data breaches and hacks. *See id.* ¶ 63.

Plaintiffs are six organizations suing on behalf of their members, clients, and program participants in Illinois who have uploaded images of themselves to the internet, and who have been, and continue to be, subjected to surreptitious and nonconsensual capture of their faceprints from those photographs by Clearview. *Id.* ¶¶ 11–15, 45–47. These individuals—including survivors of domestic violence and sexual assault, undocumented immigrants, current and former sex workers, individuals who regularly exercise their constitutional rights to protest and access reproductive healthcare services, and others—have particular reasons to fear the loss of privacy, anonymity, and security caused by Clearview's practices. *Id.* ¶¶ 34–36, 38. For example, Plaintiff Mujeres Latinas en Acción provides services to survivors of domestic violence and sexual assault, and many of its program participants are undocumented immigrants. *Id.* ¶ 38.

By divesting these individuals of control over and security in their sensitive biometric

identifiers and threatening to make it trivially easy to identify and track them both online and in the physical world, Clearview's system exposes them to stalking, harassment, and violence. *Id.* ¶¶ 34–36, 38. Clearview's conduct raises precisely the concerns with widespread surreptitious capture of biometric identifiers that motivated passage of BIPA a dozen years ago. *Id.* ¶ 9.

STANDARD OF REVIEW

Clearview does not specify the civil code section under which it has filed its motion, but it appears to raise arguments under both 735 ILCS 5/2-615 and 735 ILCS 5/2-619.[1] Such motions "admit all well-pleaded facts together with all reasonable inferences that can be gleaned from those facts." *Benton v. Little League Baseball, Inc.*, 2020 IL App (1st) 190549, ¶ 28. "A motion to dismiss pursuant to section 2-615 attacks the legal sufficiency of the complaint, and the essential question is whether the allegations of the complaint, when construed in the light most favorable to the plaintiff, are sufficient to establish a cause of action upon which relief may be granted." *Id.* "A section 2-619 motion, on the other hand, raises defects or defenses that negate plaintiff's cause of action completely[.]" *Id.* While the parties can introduce matters outside of the pleadings solely regarding personal jurisdiction, "any conflicts in the pleadings and affidavits must be resolved in the plaintiff's favor." *Russell v. SNFA*, 2013 IL 113909, ¶ 28.

ARGUMENT

I. Clearview is subject to personal jurisdiction in Illinois.

This Court has specific jurisdiction over Clearview. In Illinois, to establish specific jurisdiction, a plaintiff need only allege that (1) the defendant has sufficient "'minimum contact'

---

[1] Plaintiffs note that 735 ILCS 5/2-619.1 requires defendants who file a combined motion to specify which code section applies to each part of the motion. *See Howle v. Aqua Illinois, Inc.*, 2012 IL App (4th) 120207, ¶ 73 ("trial courts should not—and need not—accept for consideration combined motions under section 2–619.1 that do not meet these statutory requirements" and "should *sua sponte* reject such motions[.]").

with Illinois such that there was 'fair warning' that the nonresident defendant may be haled into an Illinois court[,]" (2) "the action arose out of or related to the defendant's contacts with Illinois[,]" and (3) "it is reasonable to require the defendant to litigate in Illinois." *Morgan, Lewis & Bockius LLP v. City of E. Chicago*, 401 Ill. App. 3d 947, 954 (1st Dist. 2010).

Here, as alleged in the Complaint and as evidenced by the Declarations of Freddy Martinez and Nathan Freed Wessler and their accompanying exhibits, Clearview has extensive contacts with Illinois, those contacts relate to Plaintiffs' cause of action, and it is reasonable to require Clearview to litigate in Illinois. As an Illinois federal court recently held, Clearview is subject to suit in Illinois for BIPA violations because "t[aking] biometric information from Illinois residents, creat[ing] a surveillance database, and then market[ing] and s[elling] licenses to use this database to entities in Illinois" suffices to establish personal jurisdiction in Illinois. *Mutnick v. Clearview AI, Inc.*, No. 20C0512, 2020 WL 4676667, at *2 (N.D. Ill. Aug. 12, 2020).

A. Clearview has contracted to—and did—sell access to its biometric database in Illinois, which is sufficient for jurisdiction.

Clearview has extensive contacts with Illinois. The company has provided its faceprint database to more than 105 public and private entities in Illinois, ranging from the Springfield, Naperville, and Chicago police departments, to the Illinois Secretary of State's office, to the Chicago Cubs. Compl. ¶ 62; Decl. of Nathan Freed Wessler, Ex. 1 and attached Exs. A–C; Decl. of Freddy Martinez, Ex. 2 and attached Exs. A–B. Clearview has facilitated thousands of searches of its database by these Illinois entities. Compl. ¶ 62 (Macon County Sheriff's Office and Naperville Police Department searched Clearview's database a combined 3,700 times); Wessler Decl. Ex. A at 12 (Illinois Secretary of State's office has "clock[ed] nearly 9,000 [face recognition] scans"—the second most of any Clearview user).

Clearview acknowledges that it has a significant number of in-state contacts, but contends they are irrelevant. As Clearview sees things, Plaintiffs' claim that Clearview collected Illinoisans' biometric identifiers in violation of BIPA is "[un]related to" why Clearview went to the trouble of collecting those identifiers—selling access to them to make money. But the Illinois Supreme Court has observed that the standard for what is "related to" conduct giving rise to a suit is "lenient or flexible[,]" and should be interpreted in view of a defendant's business as a whole. *Russell v. SNFA*, 2013 IL 113909, ¶ 83.

In *Russell*, a plaintiff's estate brought a wrongful death suit after a helicopter crash, naming as the defendant a French company (SNFA) that manufactured a custom bearing used in the helicopter. *Id.* ¶ 1. The helicopter was manufactured in Italy, and SNFA had no direct contacts with Illinois for helicopter bearings—they merely provided them to a global distributor. *Id.* ¶¶ 5–6. SNFA's only contact with Illinois involved bearings for fixed-wing aircrafts, which it contended was unrelated to the at-issue helicopter bearings. *Id.* ¶¶ 15, 82. Our Supreme Court held that the business, "manufacturing custom-made bearings for the aerospace industry," should be viewed as a whole, and therefore concluded that SNFA's Illinois contacts were related to the plaintiff's claim. *Id.* ¶ 84; *see Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 479 (1985) (establishing minimum contacts entails looking at "prior negotiations and contemplated future consequences, along with the terms of the contract and the parties' actual course of dealing").

Here, Clearview's Illinois-connected conduct is far more closely related to Plaintiffs' claim: the very business Clearview sought (and obtained) in Illinois was premised on the nonconsensual collection of biometric identifiers. As the Complaint makes clear, Clearview's capture of Illinoisans' faceprints, consolidation of those faceprints in a massive database, and offer of that database for sale to Illinois entities is a single course of conduct—the contracts for

sale of biometric data are more related to Clearview's illegal collection of that data than SNFA's contract to sell airplane bearings was to helicopter bearings sold separately through a distributor. Compl. ¶¶ 6–8; *see Mutnick*, 2020 WL 4676667, at *2. Without a plan to sell access to Illinoisans' faceprints, Clearview would not have captured them—and, without capturing them, Clearview could not have successfully sold its database in Illinois. *See* Compl. ¶¶ 46, 51, 62; Martinez Decl. Ex B at 45 (map showing Clearview's service areas, including Illinois). Clearview's contracts in Illinois are related to the case, and provide Clearview with more than fair warning that it will have to answer for BIPA violations here.[2]

This analysis shows why *Gullen v. Facebook.com, Inc.*, No. 15 C 7681, 2016 WL 245910 (N.D. Ill. Jan. 21, 2016), on which Clearview relies, does not help Clearview. There, the court held that there was "no relationship" between Facebook's general sales and marketing activities in Illinois, and its face recognition technology. *Id.* at *2. Here, of course, Clearview's faceprint database is the very product being marketed and sold in Illinois.

B. Clearview also targeted Illinois in other ways.

Clearview's efforts to advertise in Illinois also provide a basis for personal jurisdiction. Clearview protests that its marketing efforts were national, and never targeted Illinois. Def. Br. at 8–9. But "There is no per se requirement that the defendant especially target the forum in its business activity; it is sufficient that the defendant reasonably could foresee that its product would be sold in the forum." *Curry v. Revolution Labs., LLC*, 949 F.3d 385, 399 (7th Cir. 2020).

[2] Clearview also says that the contracts have been discontinued, but that is not relevant—personal jurisdiction attaches when the claim arises. *United Phosphorus, Ltd. v. Angus Chem. Co.*, 43 F. Supp. 2d 904, 908 (N.D. Ill. 1999). Otherwise, a defendant could evade jurisdiction by withdrawing from a state *post hoc*, as Clearview is trying to do here.

In any event, Clearview *did* directly market its face recognition database in Illinois.[3] Compl. ¶ 62. For example, between December 2019 and March 2020, Clearview sent a Springfield Police Officer who was using its product on a trial basis a series of emails that: touted Clearview's supposed accuracy and reach, Martinez Decl. Ex. B at 26; encouraged the officer to use Clearview without constraint, *id.* at 23, 25; urged him to convince other officers to use it, *id.* at 25; answered his questions about how to convert his free trial account into a permanent paid one, *id.* at 19; encouraged him to get the police department to buy Clearview's service, *id.* at 5, 25; offered a discount for bulk purchases, *id.* at 19; and offered a one-on-one video demonstration, *id.* at 21. Clearview also sent him a variety of promotional materials, including pricing information and purported data about accuracy. *Id.* at 28–46. Clearview also sent him a map showing Clearview's service areas, which expressly includes Illinois. *Id.* at 45.

Clearview similarly marketed its faceprint database to the Chicago Police Department, Martinez Decl. Ex. A; Wessler Decl. Ex. B, and the Illinois Secretary of State's office, including by negotiating a price, and offering to "help your agency" with a new feature of Clearview's service, Wessler Decl. Ex. C at 45. The company also sent multiple emails to a listserv of Illinois "fraud, loss prevention, and law enforcement professionals" advertising a free trial and touting the benefits of its system, Martinez Decl. ¶ 6, Ex. C, and met with representatives of Illinois law enforcement agencies at a trade conference to market its product, Wessler Decl. Ex. D.

These directed marketing communications constitute sufficient contacts to confer jurisdiction. *See, e.g.*, *Zazove v. Pelikan, Inc.*, 326 Ill. App. 3d 798, 805–06 (1st Dist. 2001);

[3] Plaintiffs' Complaint, declarations, and exhibits contradict Clearview's assertion to the contrary in ¶ 6 of the Schwartz Declaration. *See infra*. On a motion to dismiss for lack of personal jurisdiction, "any conflicts in the pleadings and supporting affidavits will be resolved in the plaintiff's favor." *Aspen Am. Ins. Co. v. Interstate Warehousing, Inc.*, 2017 IL 121281, ¶ 12.

Adams ex rel. Adams v. Harrah's Maryland Heights Corp., 338 Ill. App. 3d 745, 750 (5th Dist. 2003); *Dixon v. GAA Classic Cars, LLC*, 2019 IL App (1st) 182416, ¶ 16. As noted above, that the company also sold its database and captured faceprints of people in other states is immaterial. Clearview "wants to have its cake and eat it, too: it wants the benefit of a nationwide business model with none of the exposure." *Illinois v. Hemi Grp., LLC*, 622 F.3d 754, 760 (7th Cir. 2010).

For similar reasons, contrary to Clearview's assertion, this is not a case involving the mere operation of an "interactive website[.]" Def. Br. at 7. "[T]he website *in aggregate with* the contractual relationship[s] into which [Clearview] entered . . . constitutes conduct purposefully directed toward this state." *Innovative Garage Door Co. v. High Ranking Domains, LLC*, 2012 IL App (2d) 120117, ¶¶ 27, 32 (emphasis added). Nor is it like the cases Clearview cites as its best authority, which involve attempts to invoke jurisdiction in Illinois based on contacts with and events in *other* states. *See* Def. Br. at 8–10 (citing *Zamora v. Lewis*, 2019 IL App (1st) 181642, ¶ 69–70 (fire in Maine), and *Bray v. Lathem Time Co.*, No. 19-3157, 2020 WL 1492742, at *3–4 (C.D. Ill. Mar. 27, 2020) (timeclock moved to Illinois by employer)). Here, Clearview expressly targeted Illinois with advertising and marketing, and directly sold its product to buyers in Illinois.

C. It is reasonable to litigate this case in Illinois.

With regard to the third personal jurisdiction factor, Clearview does not even argue that it is unreasonable for it to litigate in Illinois, for good reason: "[W]hen a defendant enters the forum state in furtherance of a business transaction, it is not unreasonable or unduly burdensome to require the defendant to return and litigate there." *Morgan, Lewis & Bockius LLP*, 401 Ill. App. 3d at 956 (citation omitted). Because Clearview's "sales are inextricably linked to the alleged tortious activity underlying [Plaintiffs'] claims[,]" *Curry*, 949 F.3d at 401, there is

nothing "random, fortuitous, or attenuated" about Clearview facing suit in Illinois court. *Burger King Corp.*, 471 U.S. at 475 (internal quotation marks and citation omitted).

II. Illinois is allowed to regulate Clearview's violation of the rights of Illinois citizens.

A. Applying BIPA to Clearview does not violate extraterritoriality principles.

Illinois courts have adopted a "long-standing rule of construction" that a statute is "without extraterritorial effect" unless the text clearly indicates otherwise. *Avery v. State Farm Mut. Auto Ins. Co.*, 216 Ill. 2d 100, 184–85 (2005). While Clearview is correct that BIPA contains no such indication, the text makes clear that the General Assembly was specifically concerned about "national corporations" collecting Illinoisans' biometric identifiers for "new applications" of biometric technologies—precisely the conduct at issue here. 740 ILCS 14/5(b). As one federal appellate court has noted, "it is reasonable to infer [from these findings] that the General Assembly contemplated BIPA's application to individuals who are located in Illinois, even if some relevant activities occur outside the state." *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1276 (9th Cir. 2019). Thus, the legislature viewed the application of BIPA to the faceprints of Illinois residents as occurring in Illinois.

Courts have agreed that applying BIPA to the capture of biometric identifiers from Illinois residents' images uploaded to the internet from Illinois does not present an extraterritoriality problem. *In re Facebook Biometric Info. Privacy Litig.*, 326 F.R.D. 535, 547 (N.D. Cal. 2018); *see also Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1101–02 (N.D. Ill. 2017) (finding that similar circumstances "tip toward a holding that the alleged violations primarily happened in Illinois"). Similarly, here, images of Plaintiffs' members on the internet were almost certainly created in and uploaded from Illinois. Plaintiffs each have hundreds or thousands of members in Illinois, whose faceprints have likely been captured by Clearview from images

created in and uploaded from Illinois. Compl. ¶¶ 11–15, 45. For instance, ACLU member Kenneth L. Page appears online in photos taken at events hosted by the ACLU of Illinois in Springfield, and Page's central Illinois church. *Id.* ¶ 45(i). It would strain credulity to suggest that these images were not created in or uploaded to the internet from Illinois.

Moreover, as the Complaint explains and Clearview highlights in declarations, Clearview has attempted to stop collecting images uploaded from Illinois—a step that would be necessary only if Clearview had been collecting images from Illinois. *Id.* ¶ 48. It is reasonable to infer that, of the many millions of images uploaded by Illinoisans and collected by Clearview, many were uploaded from Illinois. *See id.* ¶ 44. Further, as noted above, Clearview used the biometric identifiers captured from these images to market its services to Illinois entities. *Id.* ¶¶ 60, 62–63. These entities undoubtedly used Clearview to search for Illinois residents.

Clearview suggests that because it uses servers outside of Illinois, BIPA cannot apply here. Def. Br. at 12. But that position has been rejected by every court to consider it. *See, e.g.*, *Patel*, 932 F.3d at 1276. Moreover, it misapprehends the right at issue: "[t]he Act vests in individuals and customers the right to control their biometric information by requiring notice before collection and giving them the power to say no by withholding consent." *Rosenbach*, 2019 IL 123186, ¶ 34. BIPA thus requires notice provided *in Illinois* and consent received *from Illinois*. The location of Clearview's servers is immaterial to the location of the violation. Furthermore, a server-centric interpretation would lead to absurd results, allowing server location to override the policy choices of every other state that has sought to protect its own residents.

In any event, *Avery* holds that the extraterritoriality inquiry is not subject to a "bright-line test[,]" and that each case must be decided on its own facts. 216 Ill. 2d at 187. As the Seventh Circuit has said, *Avery*'s standard "gives the trier of fact substantial latitude." *Morrison v. YTB*

Int'l, Inc., 649 F.3d 533, 538 (7th Cir. 2011). And extraterritoriality is an issue better decided on a fully developed record. *See, e.g.*, *Monroy v. Shutterfly, Inc.*, No. 16 C 10984, 2017 WL 4099846, at *6 (N.D. Ill. Sept. 15, 2017). At this stage, it is enough that the Complaint "does not *defeat* application of Illinois law." *Morrison*, 649 F.3d at 538 (emphasis in original). Clearview's motion should not be granted "unless it is clearly apparent that no set of facts can be proved that would entitle the plaintiff to relief." *Jorgenson v. Berrios*, 2020 IL App (1st) 191133, ¶ 21. Clearview has not met that standard with respect to extraterritoriality here.

B. Applying BIPA to Clearview does not violate the dormant Commerce Clause.

Relatedly, Clearview seeks dismissal under the U.S. Constitution's dormant Commerce Clause because it contends that Plaintiffs' claim seeks to apply "BIPA to Clearview's conduct in New York." Def. Br. at 14. This is incorrect, and fails to identify a dormant Commerce Clause problem. "Dormant Commerce Clause doctrine applies only to laws that *discriminate* against interstate commerce, either expressly or in practical effect." *Park Pet Shop, Inc. v. City of Chicago*, 872 F.3d 495, 501 (7th Cir. 2017). Plaintiffs allege that Clearview has failed to provide notice of its conduct or obtain consent from affected individuals *in Illinois*. BIPA does not prohibit the capture of faceprints altogether—it only prohibits such capture without notice and consent from affected Illinoisans. 740 ILCS 14/15(b). Nor does BIPA regulate Clearview's out-of-state conduct. Requiring Clearview to obtain informed consent from Illinoisans has no direct effect on Clearview's ability to capture the biometric identifiers of residents of other states or from images created in and uploaded to the internet from other states. *See, e.g.*, *Int'l Dairy Foods Ass'n v. Boggs*, 622 F.3d 628, 634 (6th Cir. 2010) (finding Ohio food-labeling rules did not impermissibly regulate out-of-state processors).

Nevertheless, Clearview suggests that "inconsistent obligations" can arise when one state

regulates certain conduct and another declines to—for example, New York, which lacks BIPA-like legislation. Def. Br. at 2, 14. But complying with Illinois law in Illinois and New York law in New York does not result in inconsistent obligations. Indeed, the same argument was raised and rejected in *In re Facebook Biometric Information Privacy Litigation*: "Facebook says that the Commerce Clause 'precludes Illinois from overriding the decisions of California and other states' to not regulate biometric information, . . . but there is no risk of Illinois law overriding the laws of the other states. This suit involves Facebook's conduct with respect to Illinois users only[.]" *In re Facebook Biometric Info. Privacy Litig.*, No. 3:15-CV-03747-JD, 2018 WL 2197546, at *4 (N.D. Cal. May 14, 2018).

Clearview relies on *Midwest Title Loans, Inc. v. Mills*, 593 F.3d 660, 667–68 (7th Cir. 2010), but it is inapplicable here. The law at issue in that case stated that a loan to an Indiana resident occurred in Indiana if the creditor advertised in Indiana, even if the Indiana resident entered into the transaction in another state. *Id.* at 662. The Seventh Circuit struck the law down because it directly regulated transactions occurring in other states by defining them as occurring in Indiana. *Id.* at 666–68. But BIPA does not regulate the nonconsensual capture of faceprints in other states. Moreover, accepting Clearview's position would inflict precisely the evil it purports to decry, by imposing New York (and other) law on conduct occurring in Illinois.

Finally, Clearview argues that any injunction issued in this case would violate the dormant Commerce Clause, but Clearview's concerns on this point are premature. *See Carle Found. v. Cunningham Twp.*, 2017 IL 120427, ¶ 34 (constitutional issues should be addressed "only if necessary"). Whether and how Clearview can comply with any injunction is a question that should be answered on a fuller record, once the parties and the Court have a better understanding of Clearview's technology. *Monroy*, 2017 WL 4099846, at *8 (noting that "after

further development of the factual record" regarding "how Shutterfly's technology works[,]" it was "conceivable" that the defendant might succeed on its dormant Commerce Clause challenge). This is simply not an issue that can or should be resolved on the pleadings.[4]

III. The First Amendment does not bar Plaintiffs' claim.

Likening itself to a search engine that merely republishes publicly-available information, Clearview next suggests that its conduct is immune from regulation under the First Amendment. But this lawsuit challenges Clearview's conduct, not its speech. Clearview can gather information from the public internet and it can run a search engine without violating BIPA. What it cannot do is capture the faceprints, or "scan[s] of . . . face geometry," 740 ILCS 14/15, of Plaintiffs' members and countless other Illinoisans without their knowledge or consent.

A ruling in Clearview's favor on this point would make it virtually impossible for the state to enact privacy and information security laws. Proper application of the First Amendment does not produce this result.[5] Indeed, the Illinois Supreme Court recently rejected a First Amendment challenge to another law in part because accepting it "would cast doubt on the constitutionality of . . . statutes that protect the privacy rights of Illinois residents[,]" specifically including BIPA. *People v. Austin*, 2019 IL 123910, ¶ 50.

A. BIPA, including as applied to Clearview, satisfies the First Amendment as a regulation of conduct subject to intermediate scrutiny under *United States v. O'Brien.*

Clearview argues that because it is using public information to generate biometric

---

[4] In addition, Clearview states that it has taken steps to ensure that BIPA does not apply to its operations, casting doubt on any dormant Commerce Clause problem here. Def. Br. at 1.

[5] As the briefs of amici curiae Electronic Frontier Foundation and First Amendment scholars demonstrate, multiple First Amendment rationales lead to this same outcome: BIPA's application to Clearview's conduct is subject to no more than intermediate scrutiny, and survives such scrutiny.

identifiers, its capture of faceprints is necessarily speech that cannot be subject to a consent requirement. But to accept this argument would be to hold that collecting fingerprints in public places or generating DNA profiles from skin cells shed in public is unregulatable speech. That contention is so outlandish that it has not, to Plaintiffs' knowledge, ever been raised in prior cases. *Cf. Rosenbach*, 2019 IL 123186, ¶ 33 (holding that nonconsensual collection of fingerprints violates BIPA).

All "biometrics" are signifiers that are used to identify people based on their unique physical and biological characteristics. Compl. ¶¶ 1, 19. "Faceprints" rely on facial-feature data, such as the distance between one's eyes and nose, and the shape of one's cheekbones. *Id.* ¶¶ 2, 20. Faceprints can be used, just like fingerprints or DNA, to discern identity. *Id.* ¶¶ 22, 52.

Far from likening the capture of a faceprint to the expression of an opinion, courts have recognized that the nonconsensual capture of a person's biometric identifier is akin to "an act of trespass[,]" *Bryant v. Compass Grp. USA*, *Inc.*, 958 F.3d 617, 624 (7th Cir. 2020), and that "an invasion of an individual's biometric privacy rights has a close relationship to" traditional privacy torts, *Patel*, 932 F.3d at 1273 (internal quotations omitted). Such activity is, and always has been, the subject of rules about consent.

The U.S. Supreme Court has recognized that this holds even for conduct—like "stealing documents or private wiretapping"—that "could provide newsworthy information[.]" *Branzburg v. Hayes*, 408 U.S. 665, 691 (1972). *See also Bartnicki v. Vopper*, 532 U.S. 514, 523, 526–27, 529–30 (2001) (recognizing that the "willful[] intercept[ion of] . . . any wire or oral communication" is "unlawful conduct"). While BIPA's notice-and consent requirement may have an incidental effect on Clearview's speech (if this Court accepts that it burdens Clearview's ability to use faceprints to express its opinion about who appears in a photograph), "it does not

necessarily follow that [nonconsensual capture of a faceprint] is constitutionally protected activity." *United States v. O'Brien*, 391 U.S. 367, 376 (1968).

When "'speech' and 'nonspeech' elements are combined in the same course of conduct, a sufficiently important governmental interest in regulating the nonspeech element can justify incidental limitations on First Amendment freedoms." *Id.*; *see also Turner Broad. Sys., Inc. v. F.C.C.*, 512 U.S. 622, 636 (1994) (applying *O'Brien* scrutiny to FCC rules that governed how "[c]able programmers and cable operators engage in and transmit speech"); *People v. Melongo*, 2014 IL 114852, ¶ 27 (same for Illinois eavesdropping statute). BIPA's requirement that entities obtain consent before capturing faceprints—including as applied to Clearview in this case—is a regulation of conduct that is subject to intermediate scrutiny under *O'Brien*.

Clearview argues that BIPA squarely regulates speech because it prevents Clearview from republishing publicly-available photographs. But BIPA does not regulate the republication of photographs; the notice-and-consent restriction that it imposes is *not* on the downstream dissemination or discussion of information Clearview has lawfully acquired, but rather on the capture of a wholly new category of information. Clearview's arguments elide the significant difference between republishing a public photograph and capturing a faceprint. To ignore this difference would be to hold that publishing a photograph of people's hands should be treated no differently than collecting their fingerprints.

Information that is posted or exposed publicly is not the same as all information that might be acquired from it through additional action—including the capture of biometric identifiers. *Cf. Kyllo v. United States*, 533 U.S. 27, 35–37 (2001) (holding that the use of infrared cameras on the exterior of a house was a Fourth Amendment search and expressly rejecting the argument that inferences drawn from publicly-available information cannot be searches). Courts

have frequently recognized this difference when it comes to biological material. Even where, as Clearview argues is the case here, "one has consented to" share certain information about one's biology—be it a photograph, "a general medical examination[,]" or "blood or urine samples"—that "does not abolish one's privacy right not to be tested for intimate, personal matters." *Norman-Bloodsaw v. Lawrence Berkeley Lab.*, 135 F.3d 1260, 1270 (9th Cir. 1998); *see also Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 616–17 (1989). Likewise here, even if Plaintiffs have consented to publication of photographs picturing them, they retain their privacy interests in their faceprints: the product of additional conduct performed on those photographs.[6]

Clearview's search engine analogy is equally unconvincing. Just as BIPA does not prohibit the republication of photographs, BIPA does not prohibit running a search engine—it merely prevents nonconsensually capturing faceprints, regardless of how they might subsequently be used. Clearview's conduct is limited only by BIPA's requirements of notice and consent; this case does not raise the specter of a ban on speech. Cases like *Jian Zhang v. Baidu.com Inc.*, relied upon by Clearview, are thus inapposite, as they are concerned with a search engine's ability to make "editorial judgments" in determining what publicly-available content to present—an issue that BIPA just does not regulate. *See* 10 F. Supp. 3d 433, 439 (S.D.N.Y. 2014). Even recognizing that BIPA may impose an incidental burden on Clearview's search tool, the law need only survive *O'Brien* scrutiny.

---

[6] For this same reason, Clearview's argument that once "truthful information is publicly revealed . . . a court may not constitutionally restrain its dissemination" also does not apply. *In re Minor*, 205 Ill. App. 3d 480, 491 (4th Dist. 1990), *aff'd,* 149 Ill. 2d. 247 (1992). Plaintiffs object to Clearview's nonconsensual capture of their faceprints—not its publication of photographs. And Clearview's reliance on *In re Minor* is particularly misplaced. Far from holding that a court could not restrain the media from publishing a minor's identity once that information is revealed, the court held that a court *could* prohibit such publication if the news obtained that information "from the courtroom" (where it is covered by a confidentiality order) rather than "through common reportorial techniques[.]" *Id.* at 491–92.

B. BIPA survives *O'Brien* scrutiny.

Under *O'Brien*, a regulation of conduct that incidentally burdens speech does not violate the First Amendment if the regulation "is within the constitutional power of the Government[,]" "if it furthers an important or substantial governmental interest [that] . . . 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." *O'Brien*, 391 U.S. at 377. Here, BIPA is plainly within Illinois's power to enact, furthers substantial governmental interests in privacy and information security, and burdens Clearview's speech no more than is necessary to further those legitimate interests.

1. Illinois has the power to regulate the capture of biometric identifiers.

BIPA "is designed to protect consumers against the threat of irreparable privacy harms, identity theft, and other economic injuries[.]" *Bryant*, 958 F.3d at 619; *see also Rosenbach*, 2019 IL 123186, ¶ 33. Clearview does not contest the state's power to enact such a law.

2. BIPA furthers substantial governmental interests.

BIPA's notice-and-consent regime furthers the state's substantial interests in protecting its residents' privacy and security. Once a faceprint is captured, a company can use it to "identify [the] individual in any of the other hundreds of millions of photos uploaded [online] each day, as well as determine when the individual was present at a specific location[,]" *Patel*, 932 F.3d at 1273. Indeed, "Clearview's mobile application . . . contains code that can pair its face recognition technology with other technology—like augmented-reality glasses—which could potentially identify every person the wearer sees walking through a neighborhood." Compl. ¶ 58. Maintaining this privacy is an important state interest because, as the General Assembly found, biometric identifiers "are biologically unique to the individual; therefore, once compromised, the

individual has no recourse [and] is at heightened risk for identity theft[.]" 740 ILCS 14/5(c); *see Rosenbach*, 2019 IL 123186, ¶ 34 (biometrics "cannot be changed if compromised or misused.").

In addition, biometric identifiers are used to enable access to other secure locations or information, including "to unlock the face recognition lock on [an] individual's cell phone[,]" *Patel*, 932 F.3d at 1273, to keep time records at work, *Miller v. Sw. Airlines Co.*, 926 F.3d 898, 901 (7th Cir. 2019), and to determine entry to a gated space, *Rosenbach*, 2019 IL 123186, ¶ 4. Databases of sensitive biometrics—including the one maintained by Clearview, *see, e.g.*, Compl. ¶¶ 6–7, 39—are therefore an inherent security hazard, as they can be subject to data breaches and employee misuse. Plaintiffs reasonably fear this risk with respect to Clearview's database, as Clearview has failed to protect other files from data breaches. *See id.* ¶ 63.

Moreover, by protecting Illinoisans' privacy, the state protects *their* speech and associational rights. As the Supreme Court has recognized, "[f]ear or suspicion that one's speech is being monitored by a stranger"—for example, by someone using Clearview to track faces at a protest, *see* Compl. ¶ 34—"can have a seriously inhibiting effect upon the willingness to voice critical and constructive ideas." *Bartnicki*, 532 U.S. at 533. Equally, fear of monitoring can chill protected association, including Plaintiffs' associations with survivors of sexual harm, survivors of domestic violence, and current and former sex workers. Compl. ¶¶ 35(i), 36(iv), 38(i).

Notwithstanding the unique privacy harms created by nonconsensual capture of biometric identifiers, Clearview argues that Plaintiffs lack any privacy interest in their faceprints because "individuals have no right to privacy in materials they post on the Internet." Def. Br. at 18, 22. As discussed above, this conflates photographs and faceprints, ignoring the intrusive conduct required to capture the latter, and the unique privacy and security harms of such capture.

Through BIPA, the General Assembly has properly "codified that individuals possess a

right to privacy in and control over their biometric identifiers and biometric information." *Rosenbach*, 2019 IL 123186, ¶ 33. The state's interest in such privacy protection is "of the highest order." *Bartnicki*, 532 U.S. at 518; *see also Wollschlaeger v. Governor, Fla.*, 848 F.3d 1293, 1314 (11th Cir. 2017) (en banc).

3. The government's interest in BIPA is not related to the suppression of free expression.

BIPA proscribes nonconsensual faceprinting because it presents a privacy and security risk—not "*because* it has expressive elements." *Texas v. Johnson*, 491 U.S. 397, 406 (1989). Clearview remains free to discuss the topic of identity and to express its opinion regarding who appears to be in a photograph, regardless of what that opinion may be. *See, e.g.*, *Clark v. Cmty. for Creative Non-Violence*, 468 U.S. 288, 295 (1984) (upholding camping ban, though it burdened protests). Conversely, even if Clearview did not speak at all, and simply captured faceprints and amassed a massive, insecure database, it would violate BIPA.

Clearview's argument that BIPA is nevertheless content-based because it "ha[s] the purpose and/or practical effect of burdening speech by reducing the effectiveness of its content" is incorrect. *See* Def. Br. at 21. Clearview relies on two cases for this point—*Sorrell v. IMS Health Inc.* and *R.A.V. v. City of St. Paul*—but neither stands for it. In *Sorrell,* the Supreme Court struck down a statute not because it diminished the effectiveness of speech, but because it "diminish[ed] the effectiveness of [speech]" *by a particular category of speakers* who "convey[ed] messages that are often in conflict with the goals of the state." 564 U.S. 552, 565 (2011). Similarly, in *R.A.V.*, the Supreme Court noted that the government could not regulate the use of sound trucks "*based on hostility—or favoritism—towards the underlying message* expressed." 505 U.S. 377, 386 (1992) (emphasis added). Thus, both cases stand only for the uncontroversial point that regulations that diminish the efficacy of speech in a content- or

viewpoint-based manner are presumptively unconstitutional. BIPA, on the other hand, broadly proscribes nonconsensual faceprinting, without respect to how the faceprints may ultimately be used. *See Sorrell*, 564 U.S. at 573 (recognizing that a First Amendment challenge to a more coherent privacy policy "would present quite a different case").[7]

Clearview also cites to *Reed v. Town of Gilbert* to argue that BIPA is facially content-based—but BIPA does not "target speech based on its communicative content[,]" nor does it "appl[y] to particular speech because of the topic discussed or the idea or message expressed." *Reed v. Town of Gilbert, Ariz.*, 576 U.S. 155, 163 (2015). Indeed, the provisions of BIPA at issue here do not facially regulate the communication of any message at all. As noted above, BIPA does not prevent Clearview from opining about who appears in a photograph, or republishing photos already available online. Instead, BIPA applies to a category of conduct—the capture of biometric identifiers—and asks only whether that capture was effected without consent.

4. The incidental restriction on speech is no greater than is essential to further the government's interest.

Finally, the state's substantial interests in BIPA "would be achieved less effectively in the law's absence and the law does not burden substantially more speech than is necessary to further the government's objective." *City of Chicago v. Alexander*, 2015 IL App (1st) 122858-B, ¶ 39, *aff'd*, 2017 IL 120350 (marks and alterations omitted); *see also Turner*, 520 U.S. at 641–42.

To further Illinois's interest in protecting individuals' privacy and security, BIPA requires that entities give notice to and obtain consent from individuals before capturing their

[7] Indeed, many of the regulations that courts have upheld under *O'Brien* regulate the efficiency of a speaker's expression. For example, must-carry provisions prevent cable operators from allowing only a small subset of speakers to monopolize broadcasts. *Turner*, 512 U.S. at 661–63. Similarly, the First District Appellate Court has held that an ordinance limiting sound volume—clearly a tool for efficiency of communication—is content neutral. *People v. Arguello*, 327 Ill. App. 3d 984, 989 (1st Dist. 2002).

faceprints. 740 ILCS 14/15(b). This "insure[s] that individuals' and customers' privacy rights in their biometric identifiers and biometric information are properly honored and protected to begin with, before they are or can be compromised," which is essential in light of the "difficulty in providing meaningful recourse once a person's biometric identifiers or biometric information has been compromised." *Rosenbach*, 2019 IL 123186, ¶ 36. "To require individuals to wait until they have sustained some compensable injury . . . before they may seek recourse . . . would be completely antithetical to the Act's preventative and deterrent purposes." *Id.* ¶ 37.[8]

Even though "a regulation need not be the least restrictive or least intrusive means of [achieving the stated governmental interest]" to satisfy intermediate scrutiny, *Alexander*, 2015 IL App (1st) 122858-B, ¶ 39, BIPA's notice-and-consent requirement targets "[t]he precise harm the Illinois legislature sought to prevent" *Rosenbach*, 2019 IL 123186, ¶ 34. Much like the ban on destroying draft cards at issue in *O'Brien*, BIPA "prohibits [the harmful] conduct and does nothing more." 391 U.S. at 381–82.

The law does not burden substantially more speech than necessary for two reasons. First, its prohibition is limited to conduct. It does not target Clearview's expression of opinion about who is pictured in a photograph. And, as the Illinois Supreme Court has noted, "whatever expenses a business might incur to meet the law's requirements are likely to be insignificant compared to the substantial and irreversible harm that could result if biometric identifiers and information are not properly safeguarded; and the public welfare, security, and safety will be advanced. That is the point of the law." *Rosenbach*, 2019 IL 123186, ¶ 37. Second, rather than impose an absolute ban on faceprinting, it allows faceprinting with an individual's consent.

---

[8] Illinois is among several states to recognize the importance of protecting biometric identifiers *before* they can be compromised. *See also* Tex. Bus. & Com. Code Ann. § 503.001; Wash. Rev. Code § 19.375.020(1).

Under BIPA, "[t]here is no . . . liability for the dissemination of the very same [biometric identifier] obtained and distributed with consent." *Austin*, 2019 IL 123910, ¶ 49; *see id.* ¶ 50 ("The entire field of privacy law is based on the recognition that some types of information are more sensitive than others, the disclosure of which can and should be regulated.").[9] Applying BIPA to Clearview in this case would not violate the First Amendment.

IV. A photograph is not a "biometric identifier," but facial geometry is.

As a last gasp, Clearview contends that its faceprint-capturing conduct is not covered by BIPA because it scans photographs rather than faces "in person[.]" Def. Br. at 24–25. But Clearview collects "faceprints[,]" which rely on "facial geometries" and therefore are "scan[s] of … facial geometry" protected by BIPA. *E.g.*, Compl. ¶¶ 1–2, 6, 20–21, 31, 44, 47, 51, 69.

BIPA defines "biometric identifier" to include a "scan of . . . face geometry[,]" and further provides that "biometric identifiers do not include . . .photographs[.]" 740 ILCS 14/10. So what happens when a scan of face geometry is derived from a still image? Four federal district courts have considered this issue, and all have concluded that BIPA's protections apply. *Vance v. Int'l Business Machines Corp.*, No. 20 C 577, 2020 WL 5530134, at *3–4 (N.D. Ill. Sept. 15, 2020); *Monroy*, 2017 WL 4099846, at *3–4; *Rivera*, 238 F. Supp. 3d at 1096; *In re Facebook Biometric Privacy Info. Litig.*, 185 F. Supp. 3d 1155, 1172 (N.D. Cal. 2016). As these

[9] For the same reasons, BIPA is not overbroad. Clearview argues that BIPA is overbroad because it bars Clearview from matching published photographs with other photographs. But BIPA only bans Clearview from doing so by relying on nonconsensually captured biometric identifiers. Clearview has failed to identify protected speech that is banned by BIPA—only speech that is incidentally burdened by it. *See People v. Williams*, 235 Ill. 2d 178, 200, 203 (2009) (recognizing that "the Supreme Court has cautioned that a statute's overbreadth must be *'substantial*, not only in an absolute sense, but also relative to the statute's plainly legitimate sweep'" and holding that the speaker's offer of a narrower restriction that "would largely defeat [the state's] . . . interest" in a challenged law cannot establish overbreadth).

courts have observed, there is an "absence of any textual support" for the "in person" limitation Clearview seeks to impose. *Monroy*, 2017 WL 4099846, at *3.

The statute's definition of "biometric identifier" includes several specific *types* of biometrics but says nothing about *how* these identifiers are collected. *See* 740 ILCS 14/10. In contrast, "biometric information[,]" does specify how the information must be collected: it specifically excludes information derived from anything other than a "biometric identifier[]." *Id.* "Under our well-settled rules of statutory construction, where the legislature includes particular language in one section of a statute but omits it in another section of the same statute, courts will presume that the legislature acted intentionally in the exclusion or inclusion." *People v. Hunter*, 2017 IL 121306, ¶ 48 (internal quotation omitted). The legislature understood how to limit the scope of information protected by BIPA to data collected in certain ways. But it chose not to do so with respect to "biometric identifier[s.]" That choice must be respected. *See Rivera*, 2017 WL 748590, at *6; *In re Facebook Biometric Privacy Info. Litig.*, 185 F. Supp. 3d at 1172.[10]

And the legislature's choice makes perfect sense. Under the plain language of the statute, a biometric identifier—including a scan of face geometry—can be derived from *any* source (including a photograph). 740 ILCS 14/10. Photographs do not themselves count as biometric identifiers because, if they did, any entity operating in Illinois (like a newspaper) would violate BIPA simply by collecting photographs of people. That would be absurd.

Moreover, excluding Clearview's faceprints from BIPA simply because still images are involved would essentially gut the law because faceprints are almost always collected from still

[10] Tellingly, the legislature did *not* enact a BIPA amendment that would have limited "scan[s]" under § 10 to only "an in-person process" and excluded information pulled from a photograph from the definition of "biometric identifier." HB 6074 (2016), Senate Amdt. 1.

images.[11] Retina and iris scans also involve taking photographs of the eye. It would be absurd if, notwithstanding being included in the definition of "biometric identifier[,]" these biometrics were removed from the statute's coverage because they require the creation of still images first.

Clearview responds that all of the other "biometric identifier[s]" covered by BIPA are collected in person, so the Court should read that limitation into the statute. Def. Br. at 24 & n.13. Clearview is wrong as a factual matter.[12] But in any event, it is well-settled that a court "may not depart from a statute's plain language by reading into it exceptions, limitations, or conditions the legislature did not express." *People ex rel. Madigan v. Kinzer*, 232 Ill. 2d 179, 184–85 (2009). The definition of "biometric identifier" contains no limitation on how identifiers are collected. Because the language is clear, new limitations cannot be read into the law.

Moreover, this is a statute that explicitly deals with a fast-evolving technology: "because advances in technology are what drove the Illinois legislature to enact the Privacy Act in the first place, it is unlikely that the statute sought to limit the definition of biometric identifier by limiting how the measurements are taken." *Rivera*, 238 F. Supp. 3d at 1095–96.

CONCLUSION

For the foregoing reasons, the motion to dismiss should be denied.

---

[11] *See, e.g.*, Wendy Davis, *Illinois Privacy Law Tested By 'Faceprint' Cases*, MEDIA POST, (Aug. 6, 2015), https://www.mediapost.com/publications/article/255620/illinois-privacy-law-tested-by-faceprint- ("I have literally never heard of any facial recognition system that works off of anything other than a photo or a video still[.]") (quoting Professor Alvaro Bedoya, former chief counsel to the Senate Judiciary Subcommittee on Privacy, Technology and the Law).

[12] For example, fingerprints, iris scans, and voiceprints can be obtained from photographs or recordings. *See* Thomas Brewster, *Inside America's Secret $2 Billion Research Hub*, Forbes (July 13, 2020), https://www.forbes.com/sites/thomasbrewster/2020/07/13/inside-americas-secretive-2-billion-research-hub-collecting-fingerprints-from-facebook-hacking-smartwatches-and-fighting-covid-19/#293521ad2052 (fingerprints from photographs); *Samsung S8 'Eye Security' Fooled by Photo*, BBC News (May 23, 2017), https://www.bbc.com/news/technology-40012990 (iris scanning of photo); Compl. ¶ 46, *Zaluda v. Apple Inc.*, No. 2019-CH-11771 (Cir. Ct. Cook Cty. Oct. 10, 2019) (voiceprints from audio recordings).

Respectfully submitted,

Dated: November 2, 2020

By: /s/ Benjamin H. Richman
One of Plaintiffs' Attorneys

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, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378
Firm ID: 62075

Nathan Freed Wessler*
nwessler@aclu.org
Vera Eidelman*
veidelman@aclu.org
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, New York 10004
Tel: 212.549.2500
Fax: 212.549.2654

Attorneys for Plaintiffs American Civil Liberties Union, Chicago Alliance Against Sexual Exploitation, Sex Workers Outreach Project Chicago, Illinois State Public Interest Research Group, Inc., and Mujeres Latinas en Acción

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.
150 North Michigan Avenue, Suite 600
Chicago, IL 60601
Tel: 312.201.9740

Attorneys for Plaintiffs American Civil Liberties Union, American Civil Liberties Union of Illinois, Chicago Alliance Against Sexual Exploitation, Sex Workers Outreach Project Chicago, Illinois State Public Interest Research Group, Inc., and Mujeres Latinas en Acción

* *Admitted pro hac vice*