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 Honorable Pamela McLean Meyerson

PLAINTIFFS' SURREPLY TO DEFENDANT'S MOTION TO DISMISS

Plaintiffs here address the arguments raised by Professors Eugene Volokh, Jane Bambauer, and the First Amendment Law Clinic at Duke ("Clinic Amici") in their amicus brief supporting Clearview's motion to dismiss on First Amendment grounds. Because some of the arguments that Clinic Amici make are either correct or irrelevant, Plaintiffs limit this surreply to the brief's three erroneous arguments—which, if accepted, would represent a dangerous departure from current First Amendment jurisprudence.[1]

First, Clinic Amici urge this Court to hold that BIPA directly regulates speech, not conduct, on the theory that all acts that precede speech or involve the collection or analysis of data constitute expression. But this categorical argument reaches too far. Accepting it would mean that wiretapping, trespass, and identity theft—equally acts that involve the collection,

[1] Because Plaintiffs do not argue that faceprints or Clearview's speech constitute commercial speech on a matter of private concern, Plaintiffs do not address Clinic Amici's objections to those arguments. *See* Clinic Amici Br. at 7–10.

analysis, or use of information—are fully protected expression, not conduct. It would also cast "constitutional doubt . . . [on] virtually every form of economic regulation we have. Economic or commercial policy affecting data flows, which is to say all economic or social policy, would become almost impossible." Neil M. Richards, *Why Data Privacy Law Is (Mostly) Constitutional*, 56 Wm. & Mary L. Rev. 1501, 1507–08 (2015) (criticizing Professor Bambauer's article, *Is Data Speech?*, advancing this argument). And as Professor Bambauer herself recognizes, it would likely signal the end for privacy protections like HIPAA and the Fair Credit Reporting Act. *See* Jane Bambauer, *Is Data Speech?*, 66 Stan. L. Rev. 57, 113–14 (2014).

Radical as this argument is, it is also largely irrelevant. The vast majority of cases that Clinic Amici rely on pursuant to this theory apply intermediate scrutiny, and Plaintiffs agree that BIPA must satisfy intermediate scrutiny in this case. To convince this Court to nevertheless apply strict scrutiny, Clinic Amici next argue that BIPA is content-based because it requires consent for the faceprinting only of humans. While almost silly on an initial read, this argument, too, is imprecise and dangerous. Accepting it would subject essentially any focused regulation to strict scrutiny—including, for example, a law prohibiting the destruction of draft cards but not playing cards, *but see United States v. O'Brien*, 391 U.S. 367 (1968)—and it would push legislators to regulate far too widely in an effort to avoid such scrutiny.

Finally, Clinic Amici argue that BIPA fails even intermediate scrutiny because there is no privacy harm in comparing two images of a person's face. This misconstrues the nature of Plaintiffs' claim, which challenges the nonconsensual harvesting of private information, not the collection or comparison of public images. And it also misunderstands the harms that BIPA aims to prevent, including those that have been documented in the years since BIPA became law.

The Court need not permit Clinic Amici's take to gain steam here. Plaintiffs'

view—that BIPA is subject to *intermediate* scrutiny for its incidental burdens on speech—enjoys the support of half a century's worth of constitutional law. BIPA survives that scrutiny, and Clearview's motion to dismiss should be denied.

I. BIPA is not a direct regulation of speech.

Clinic Amici argue that because Clearview's end product is speech—that is, telling a customer who a person in a photograph is—every step in the process of producing it must be speech, too. But the First Amendment does not fully protect every act that involves the collection or analysis of data. That is not how our Constitution treats, for example, the acts of trespassing or breaking and entering. *See, e.g.*, *Lloyd Corp., Ltd. v. Tanner*, 407 U.S. 551, 568 (1972). Nor is it how we think of "stealing documents or private wiretapping," even though such acts "could provide newsworthy information"—and, like capturing faceprints, deal entirely in 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). Equally, this logic would require accepting that any use or analysis of amassed or publicly-available information is speech—yet courts do not typically view identity theft or stalking as speech. *See, e.g.*, *People v. Ashley*, 2020 IL 123989, ¶ 42 (construing stalking statute "to proscribe only unlawful conduct").[2] And, while courts have not been asked to reach these questions, they would almost certainly hold that capturing fingerprints from a photograph of a hand or deciphering a private password from asterisks shown on a public login screen is conduct, not expressive speech.

[2] Similarly, the Supreme Court has repeatedly observed that the destruction of or refusal to use certain information is conduct, not speech. *See, e.g.*, *Rumsfeld v. Forum for Acad. & Institutional Rights, Inc*., 547 U.S. 47, 66 (2006) (refusal to pay income taxes is conduct, not speech); *United States v. O'Brien*, 391 U.S. 367, 375 (1968) (same for destruction of tax books and records).

"'[H]owever complete is the right . . . to state public things and discuss them, that right, as every other right enjoyed in human society, is subject to the restraints which separate right from wrong-doing.'" *Branzburg*, 408 U.S. at 692 (quoting *Toledo Newspaper Co. v. United States*, 247 U.S. 402, 419–20 (1918)). Harvesting private information without consent is not the same as recording publicly-available information; it can cross the line into wrong-doing. A person pictured even in a publicly-available image has no reason to think that their facial geometry will be extracted from the image and used to eliminate their anonymity and security forever. The facial attributes from which a faceprint are captured may be visible, to be sure, but not all which can be harvested from that which is visible is public. *Cf. Kyllo v. United States*, 533 U.S. 27, 35–36 (2001) (recognizing that inferences drawn from publicly-available information can be searches and holding that the use of infrared cameras on the exterior of a house was a Fourth Amendment search).

Of course, some acts, including some involving data collection and analysis, can be so fundamentally intertwined with expression as to be analytically the same. *See, e.g.*, *Anderson v. City of Hermosa Beach*, 621 F.3d 1051, 1061–62 (9th Cir. 2010) ("Although writing and painting can be reduced to their constituent acts, and thus described as conduct, we have not attempted to disconnect the end product from the act of creation."); *Am. Civil Liberties Union of Illinois v. Alvarez*, 679 F.3d 583, 600 (7th Cir. 2012) ("In short, the eavesdropping statute restricts a medium of expression [photography]—the use of a common instrument of communication—and thus an integral step in the speech process"). But the conduct BIPA regulates is the nonconsensual capture of biometric identifiers, which often isn't used for expression at all. *See, e.g.*, *Miller v. Sw. Airlines Co*., 926 F.3d 898, 901 (7th Cir. 2019) (capture of biometric identifiers used to keep time records at work), *Rosenbach v. Six Flags Ent. Corp.*,

2019 IL 123186, ¶ 4 (capture of biometric identifiers used to grant entry to a gated space).[3] The non-consensual capture of faceprints does not become a medium of expression simply because it is a predicate step in Clearview's business of telling its customers who people are. Accepting Amici Clinic's recharacterization of *Anderson*, *Alvarez*, and other right-to-record cases to stand for this recursive reasoning would mean that any conduct is fully protected expression as long as the actor intends to glean information from it or later talk about it. By this logic, were Clearview to wiretap or steal the identities of the people it identifies for its customers, those acts would equally constitute expression. This proposition is contradicted by the well-established caselaw discussed above.

Clinic Amici also argue that "[t]he use of mechanical means . . . does not negate First Amendment protection for information gathering." Clinic Amici Br. at 5–6, 7. Plaintiffs agree. Plaintiffs challenge Clearview's capture of faceprints not because of the technological means that the company uses, but because of its conduct: the harvesting of biometric identifiers.[4]

II. BIPA is not subject to strict scrutiny.

Clinic Amici next argue that BIPA is a content-based regulation of speech subject to strict scrutiny because it requires consent from humans for faceprinting, but not from cats. Clinic Amici Br. at 8.

This argument would find a content-based distinction in any regulation. By Amici's logic, the Supreme Court should have applied strict scrutiny in *O'Brien* itself—which established the intermediate scrutiny standard that applies in this case—because the law at issue prohibited

[3] For the same reason, Amici's argument that BIPA is targeted at expression because privacy and security risks are expressive harms fails.

[4] Clinic Amici occasionally blur the line on the challenged conduct, implying that it is Clearview's amassing a database of photographs, rather than extracting biometric identifiers without consent, that is at issue. Clinic Amici Br. at 11. It is the latter that violates BIPA.

burning draft cards, but not playing cards. *But see* 391 U.S. at 376 (applying intermediate scrutiny). And the Supreme Court should have viewed the wiretapping notice-and-consent requirement discussed in *Bartnicki*, which applied to the dialogue of humans, but not the meowing of cats, as a content-based regulation of speech. *But see Bartnicki*, 532 U.S. at 526 (holding that statute prohibiting dissemination of communications recorded without consent was content-neutral)*; see also People v. Clark*, 2014 IL 115776, ¶ 19 (holding that Illinois eavesdropping statute is content-neutral and therefore subject to intermediate scrutiny).

Accepting Amici's logic would mean that every privacy regulation is either subject to strict scrutiny because it is content-based, or unconstitutional because it is overbroad. But courts have refused to apply strict scrutiny to, or strike down, every privacy regulation. *See, e.g.*, *Nat'l Cable & Telecomms. Ass'n v. FCC*, 555 F.3d 996, 1001–02 (D.C. Cir. 2009) (applying intermediate scrutiny to telecommunications privacy law); *Trans Union Corp. v. FTC*, 267 F.3d 1138, 1140–41 (D.C. Cir. 2001) (applying intermediate scrutiny to financial institution privacy law). As discussed at length in Plaintiffs' Opposition, BIPA does not directly regulate—nor does it seek to suppress speech about—any topic, including human identity, through its notice-and-consent requirement for capturing faceprints. *See* Pls.' Br. at 20–23.

For this reason, Amici's reliance on cases applying strict scrutiny to laws regulating the use or collection of specific types of data is also misplaced. *See* Clinic Amici Br. at 6. Amici rely most heavily on *PETA v. Stein*, but that case is inapposite. The *PETA* Court reviewed a law that prohibited the capture of employer data used to "breach a duty of loyalty" and unsurprisingly found it to be a content-based restriction—it regulated information gathering *only* when it would be used for a specific purpose. *People for the Ethical Treatment of Animals, Inc. v. Stein*, 466 F. Supp. 3d 547, 573 (M.D.N.C. 2020) ("[T]he condition imposed is based on the purpose of the

speech."). Indeed, the court held that another provision of the same law, which flatly prohibited using an unattended camera to record on the employer's premises, was content-neutral (and subject to intermediate scrutiny) even though it prohibited recording only on an employer's premises and not elsewhere. *Id.* at 574. BIPA similarly regulates "only" the capture of human biometric identifiers but does so without regard to any ultimate purpose of the capture—therefore, it is a content-neutral regulation.

Similarly, Amici are wrong to rely on *Animal Legal Defense Fund v. Otter. Otter* applied strict scrutiny to a law requiring an employer's consent before an employee could film "the conduct of an agricultural production facility's operations"—and so regulated filming "animals abused on a farm" but not "the farm owner's children." 44 F. Supp. 3d 1009, 1023 (D. Idaho 2014). In other words, the statute was designed to suppress speech about the specific topic of animal abuse. BIPA does not make such distinctions; it regulates the capture of *all* faceprints, and its application does not turn on whether Clearview's speech is about identity, security, or any other topic—nor does the law's legislative history suggest that the aim was to silence speech on any specific topic, much less any particular viewpoint, as was the case in *Otter*. *Id.* at 1024. BIPA is a content-neutral regulation of the capture of facial geometry. Thus, contrary to Amici's arguments, BIPA is subject to intermediate scrutiny.

III. BIPA survives intermediate scrutiny.

As Amici themselves note, "[t]he balance between free speech and privacy is struck by drawing a clear distinction between the collection of public information and the harvesting of private and sensitive information[.]" Clinic Amici Br. at 10. That is precisely the line drawn by BIPA's notice-and-consent requirement. As discussed at length in Plaintiffs' Opposition and above, BIPA protects the privacy and security of Plaintiffs and other Illinoisans in part because

gathering public photographs is *not* the same as capturing faceprints, and faceprints are private. *See* Pls.' Br. at 14–17.

Indeed, Amici recognize that "there are some contexts where the harms from identifying a previously unidentified person clearly outweigh the benefits," and suggest that "a narrow law prohibiting the use of facial recognition technologies near the entrance of doctor's offices or by online services offering sensitive and confidential advice . . . may comfortably fit within the reasoning of existing First Amendment precedent." Clinic Amici Br. at 13.

But this argument—meant to allay reasonable privacy fears—both proves Plaintiffs' point that publicly exposing one's face is not the same as publicly exposing a faceprint, Pls' Br. 16–17, and is impracticable. How will those attending religious services, joining in political demonstrations, or seeking medical care know whether they will be subject to invasive face recognition? What spaces—and which topics of advice—are sufficiently private? How could any law possibly account for all such circumstances—especially given the fact that one's regular movements to even non-"sensitive" locations such as homes can reveal personal, political, and professional associations? *See Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018). And, on the flipside, how will users of face recognition know if they must seek an individual's consent before capturing their faceprint? Such a policy would be impossible to implement in practice—and, accepting Amici's argument, may well turn out to be content-based. Rather, the proper solution for the security and privacy harms caused by the absence of control over one's biometric identifiers is the one provided by BIPA: a notice-and-consent requirement for the capture of a faceprint. *See* Pls.' Br. at 18–23.

Relatedly, Amici are incorrect to argue that this lawsuit "aim[s] to quash an emerging information technology before its implications and benefits are understood." Clinic Amici Br. at

13. BIPA has been on the books for more than a dozen years, and far from aiming to stifle innovation through the law, Illinois enacted BIPA to build trust in biometric technology so that innovators could further develop it. *See* 740 ILCS 14/5(a), (e), (g) (legislative findings explaining that "[t]he use of biometrics . . . appears to promise streamlined financial transactions and security screenings," but that without effective regulation, "many members of the public are deterred from partaking in biometric identifier-facilitated transactions," and that "[t]he public welfare, security, and safety will be served by regulating the collection . . . of biometric identifiers"). The legislative record demonstrates a careful balancing of interests, and one that results in a person's "power to say no" before their immutable identifiers are taken from them. *Rosenbach*, 2019 IL 123186, ¶ 34.

Moreover, we are now well into the age of face recognition, and there is nothing speculative about face recognition's harms. For example, the Chinese government is amassing facial recognition databases of individuals who have mental illnesses, used drugs, or petitioned the government with grievances, and it is using face recognition to track and oppress the Uighur population.[5] Private companies in China have likewise developed face recognition technology that can purportedly identify and track members of the Uighur minority.[6] Meanwhile, government agencies in the United States have used face recognition—including Clearview's

[5] Paul Mozur, *One-month, 500,000 Scans: How China is Using A.I. to Profile a Minority*, N.Y. TIMES (Apr. 14, 2019), https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html.

[6] Drew Harwell & Eva Dou, *Huawei Tested AI Software That Could Recognize Uighur Minorities and Alert Police, Report Says*, WASH. POST (Dec. 8, 2020), https://www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-that-could-recognize-uighur-minorities-alert-police-report-says/; *Alibaba Facial Recognition Tech Specifically Picks Out Uighur Minority – Report*, Reuters (Dec. 17, 2020), https://www.reuters.com/article/us-alibaba-surveillance/alibaba-facial-recognition-tech-specifically-picks-out-uighur-minority-report-idUSKBN28R0IR.

technology—to surveil people exercising their First Amendment rights at protests.[7] American retail chains have surreptitiously used face recognition technology to identify shoppers, often in low-income neighborhoods and communities of color, resulting in harassment of shoppers who were deemed suspicious by the technology but in fact did nothing wrong.[8] A company that marketed itself as providing an online photo storage service secretly used millions of users' photos to train a face recognition algorithm, which it then sold to other private companies and government entities.[9] These and other well-established dangers of face recognition technology have led the world's largest professional computing society, ACM, to call for "an immediate suspension of the current and future private and governmental use of facial recognition (FR) technologies in all circumstances known or reasonably foreseeable to be prejudicial to established human and legal rights" because the technology "has often compromised fundamental human and legal rights of individuals to privacy, employment, justice and personal liberty."[10]

---

[7] Justin Jouvenal & Spencer S. Hsu, *Facial Recognition Used to Identify Lafayette Square Protestor Accused of Assault*, WASH. POST (Nov. 2, 2020), https://www.washingtonpost.com/local/legal-issues/facial-recognition-protests-lafayette-square/2020/11/02/64b03286-ec86-11ea-b4bc-3a2098fc73d4story.html; Kate Cox, *Cops in Miami, NYC Arrest Protestors From Facial Recognition Matches*, ArsTechnica (Aug. 19, 2020), https://arstechnica.com/tech-policy/2020/08/cops-in-miami-nyc-arrest-protesters-from-facial-recognition-matches.

[8] Jeffrey Dastin, *Rite Aid Deployed Facial Recognition Systems in Hundreds of U.S. Stores*, Reuters (July 28, 2020), https://www.reuters.com/investigates/special-report/usa-riteaid-software/.

[9] Olivia Solon & Cyrus Farivar, *Millions of People Uploaded Photos to the Ever App. Then the Company Used Them to Develop Facial Recognition Tools*, NBC News (May 9, 2019), https://www.nbcnews.com/tech/security/millions-people-uploaded-photos-ever-app-then-company-used-them-n1003371.

[10] Press Release, Association for Computing Machinery, *ACM US Technology Policy Committee Urges Suspension of Private and Governmental Use of Facial Recognition Technologies* (June 30, 2020), https://www.acm.org/media-center/2020/june/ustpc-issues-statement-on-facial-recognition-technologies.

CONCLUSION

As described above, BIPA is subject to and satisfies intermediate scrutiny, and Clearview's Motion to Dismiss should be denied.

Respectfully submitted,

Dated: January 5, 2021

By: /s/ J. Eli Wade-Scott
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

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*

CERTIFICATE OF SERVICE

I, J. Eli Wade-Scott, an attorney, hereby certify that on January 5, 2021 I served the above and foregoing document by causing a true and accurate copy of the same to be filed and transmitted to all counsel of record via the Court's electronic filing system.

/s/ J. Eli Wade-Scott