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 Hon. Pamela McClean Meyerson

BRIEF OF AMICI LAW PROFESSORS
IN OPPOSITION TO DEFENDANT'S MOTION TO DISMISS

Craig Futterman
MANDEL LEGAL AID CLINIC
UNIVERSITY OF CHICAGO LAW SCHOOL
6020 S. University Ave.
Chicago, IL 60637
(773) 702-9611
futterman@uchicago.edu
Cook County #91074

G.S. Hans*
STANTON FOUNDATION FIRST AMENDMENT CLINIC
VANDERBILT LAW SCHOOL

131 21st Ave. So.
Nashville, TN 37206
Tel.: (615) 343-2213
gautam.hans@vanderbilt.edu

** Application for admission pro hac vice forthcoming*

November 2, 2020

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

STATUTES

OTHER AUTHORITIES

STATEMENT OF INTEREST[1]

Amici are law professors with expertise in information privacy and the First Amendment. Amici have collectively authored scores of articles, opinion pieces, and multiple books on the evolution of First Amendment doctrine and, in particular, its intersection with privacy rights.

Amici write to assist the Court by providing important context for the constitutional analysis of Illinois law. Privacy statutes commonly require individuals to consent before others may disseminate sensitive information about them. Neither the singling out of particular information for protection nor the imposition of a consent requirement transform these quotidian protections into unconstitutional censorship. Contrary to Clearview's position, Illinois' Biometric Information Privacy Act (BIPA) is not a content-based speech restriction, and the Constitution does not require that firms be able to scrape, harvest, and sell individuals' most sensitive information free of oversight or regulation by elected legislatures.

INTRODUCTION AND SUMMARY OF ARGUMENT

BIPA is a content-neutral law that regulates biometric information and identifiers, in a similar manner to multiple state and federal privacy laws. As such, and consistent with many cases analyzing such laws in the face of First Amendment challenges, it is constitutional.

BIPA does not target speech, and its regulation of one type of information does not transform it into a content-based regulation. Instead, even assuming BIPA affects speech at all, the statute is properly characterized as a content-neutral time, place, and manner restriction. Under longstanding precedent, such restrictions are subject to an intermediate scrutiny standard, which BIPA easily satisfies. And despite Clearview's contentions, its activities do not constitute

[1] Amici confirm that no party or counsel for any party authored this brief in whole or in part, that no person other than amici or their counsel made any monetary contribution intended to fund the preparation or submission of this brief, and that both parties consent to the filing of this brief.

speech. Given the early stage of this litigation and existing state and federal precedent, it would be most prudent for this court to deny Clearview's Motion to Dismiss on constitutional grounds.

ARGUMENT

I. Clearview conflates its right to collect and use publicly available photographs—a right that BIPA does not affect or hinder—with its collection of biometric information from those photographs — an activity for which BIPA requires individual consent.

In its motion, Clearview asserts that BIPA impermissibly burdens the firm's expressive rights by impeding its ability to collect publicly available photographs, transforming it into a content-based regulation. Def.'s Mem. in Supp. of Mot. to Dismiss at 16–19. This maneuver is beside the point. Clearview misstates both what BIPA regulates and the subject matter covered by the First Amendment.

BIPA regulates the collection, use, and retention of biometric identifiers, not of photographs. 740 ILCS 14/10 ("Biometric identifiers do not include… photographs."). BIPA's ambit is thus quite distinct from regulating photographs, videos, or other visual media from whence biometric identifiers are collected. In *Patel v. Facebook, Inc.*, the U.S. Court of Appeals for the Ninth Circuit described how biometric information is collected as follows by Facebook in order to facilitate facial recognition:

> the technology extracts the various geometric data points that make a face unique, such as the distance between the eyes, nose, and ears, to create a face signature or map. The technology then compares the face signature to faces in Facebook's database of user face templates (i.e., face signatures that have already been matched to the user's profiles).

932 F.3d 1264, 1268 (9th Cir. 2019). This process bears no resemblance to speech. It is a form of analysis that does not implicate Clearview's speech rights, just as any industrial process that touches on communicative material does not automatically implicate the First Amendment.

Consider, by way of analogy, the International Standard Book Number (ISBN), a unique ten-digit numerical identifier assigned to each edition of a published book that is frequently translated into a barcode. The books that bear ISBN numbers are obviously expressive works. *Joseph Burstyn, Inc. v. Wilson*, 343 U.S. 495, 501–02 (1952) ("That books, newspapers, and magazines are published and sold for profit does not prevent them from being a form of expression whose liberty is safeguarded by the First Amendment."). Bookstores frequently use barcode scanners to interpret ISBN barcodes and ring up customers' orders using a point of sale system. Insofar as an ISBN number identifies a book or monograph, it communicates a certain message, and the computational interpretation of an ISBN barcode generates information by rendering the string of numbers into text. But the bookstore employee who uses a scanner to "read" an ISBN barcode in order to record the books that the customer is purchasing could hardly be deemed to engage in First Amendment protected activity. A library that uses a barcode scanner to check out a patron's books could not thereby claim a First Amendment right to contravene statutes protecting the confidentiality of library records. Nor may the barcode scanner's manufacturer invoke the First Amendment as a shield against regulation. Yet this is precisely what Clearview's argument mandates — that any analysis of material that might be protected by the First Amendment against existing material necessarily constitutes speech on its own. This argument sweeps too broadly.

Patel also illuminates the distinction between consenting to upload photographs and consenting to the collection, use, and retention of biometric identification. Clearview contends that BIPA constrains its collection of publicly available information, though it does nothing of the sort. Def.'s Mem. in Supp. of Mot. to Dismiss at 19–20. Despite Clearview's claims, BIPA does not create a consent requirement for the collection of publicly available material, but rather

for the collection of biometric identifiers that might or might not be based on that material. 740 ILCS 14/15. Regardless of whether individuals have waived any privacy rights to the underlying media — either through consent or by appearing in public — they have not waived their rights under BIPA, which creates a subsequent consent requirement to the biometric analysis of the content Clearview analyzes.

Finally, Clearview — without evidence — argues that the Illinois legislature could not have intended to regulate faceprinting in BIPA as each of the "covered biometric identifiers describes an in-person process for obtaining information about an individual." Def.'s Mem. in Supp. of Mot. to Dismiss at 24. But in addition to in-person acquisition of "face geometry," the text of BIPA also prohibits private entities from "receiv[ing] through trade" any biometric identifiers. 740 ILCS 14/15(b) ("No private entity may collect, capture, purchase, *receive through trade*, or otherwise obtain a person's or a customer's biometric identifier or biometric information…" (emphasis added)). Clearview's argument ignores the plain text of the statute. The Illinois' legislature's inclusion of "receive through trade, or otherwise obtain" as potential sources for biometric identifiers or information demonstrates that the Illinois legislature intended to regulate entities that collect biometric information even if collection does not occur in person, and that Clearview's actions are therefore implicated by BIPA.

II. To the extent BIPA touches on speech at all, it is a content-neutral time, place, and manner restriction.

Assuming, for the sake of argument, that BIPA burdens speech at all, it is a content-neutral regulation that easily satisfies the relevant standard of intermediate scrutiny. Clearview incorrectly contends that, because BIPA limits its ability to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information" without consent, the statute is a content-based restriction that implicates its speech.

In doing so Clearview attempts to subject BIPA to strict scrutiny review, the most heightened standard of constitutional review. This maneuver ignores existing law, which — to the extent that BIPA even affects speech — properly characterizes BIPA as a content-neutral time, place, and manner restriction that withstands intermediate scrutiny.

BIPA regulates the collection, use, and retention of biometric information in order to protect information pertaining to individuals and creates a consent framework to govern the dissemination of biometric identifiers. 740 ILCS 14/15. While Clearview claims a sweeping immunity from BIPA, citing its own expressive rights, it ignores the plain text of BIPA, which does not hinge on the communicative aspect of speech. BIPA does not permit the dissemination of information by some actors but not others (as did the detailing law in *Sorrell v. IMS Health*, 562 U.S. 1127 (2011)), nor does it permit communications for some purposes but not others (as the Telephone Consumer Protection Act did, *Barr v. Am. Ass'n of Pol. Consultants, Inc.,* 140 S. Ct. 2335 (U.S. Jul. 6, 2020)). In short, BIPA does not target speech, and to the extent that it implicates Clearview (or anyone else's) speech, functions as a content-neutral time, place, and manner restriction.

Clearview wrongly contends that because BIPA targets specific "content" — biometric identifiers and information — it is content-based. Def.'s Mem. in Supp. of Mot. to Dismiss at 19. But legislative efforts to address the harms caused by the disclosure of specific, sensitive private data such as biometric information are consistent with the First Amendment. Consider the Electronic Communications Privacy Act, which prohibits the interception of wire, oral, and electronic communications and the dissemination of the contents of those communications. 18 U.S.C. § 2511. Like BIPA, ECPA singles out certain kinds of communications for privacy protections. Like BIPA, ECPA articulates statutory exceptions to its prohibitions, including

where "one of the parties to the communication has given prior consent to such interception." *Id.* § 2511(c). Faced with a constitutional challenge to this prohibition, the U.S. Supreme Court determined that the prohibition on disseminating the contents of private conversations was content-neutral, reasoning that the statutory distinctions were not "justified by reference to the content of those conversations. Rather, the communications at issue are singled out by virtue of the fact that they were illegally intercepted—by virtue of the source, rather than the subject matter." *Bartnicki v. Vopper*, 532 U.S. 514, 526 (2001). The fact that ECPA applied only to certain communications, in other words, was simply not enough to transform the statute into a content-based speech restriction.

The Illinois Supreme Court has followed this approach, recognizing that privacy laws, by definition, must make distinctions about what information might be more sensitive and thus worth of protection. *People v. Austin*, 2019 IL 123910, at *9, *cert. denied*, No. 19-1029, 2020 WL 5882221 (U.S. Oct. 5, 2020) (citing BIPA, among other laws). *Austin* upheld an Illinois statute that criminalized the nonconsensual dissemination of private sexual images. Like BIPA, the statute at issue in *Austin* both regulated only certain types of information — private sexual images — and imposed a consent requirement for dissemination. As the *Austin* Court noted, however, merely requiring consent before disseminating certain types of highly sensitive information does not transform a statute into a content-based speech restriction. So too here, BIPA's regulation of "biometric information" and "biometric identifiers" does not transform it into a content-based regulation.

BIPA's structure resembles that of the statute in *Austin*. Like that statute, it does not prohibit, but rather regulates, the dissemination of information. BIPA carefully regulates biometric identifiers and uses a consent framework to protect individual privacy. 740 ILCS

14/15(b). As the Illinois Supreme Court noted in *Austin*, finding that statute unconstitutional on First Amendment grounds would imperil multiple other Illinois statutes, including BIPA. 2019 IL 123910 at *9. This court should adopt the Illinois Supreme Court's reasoning when analyzing BIPA.

Put another way, BIPA regulates the conditions for disclosing private information about individuals rather than any expression that Clearview propounds. The Seventh Circuit has likewise concluded that privacy statutes that restrict the collection and use of private information obtained in violation of the law are consistent with the First Amendment. *Dahlstrom v. Sun-Times Media, LLC*, 777 F.3d 937, 949 (7th Cir. 2015) ("The origin of the information is thus crucial to the illegality of its publication—the statute is agnostic to the dissemination of the very same information acquired from a lawful source."). As *Bartnicki, Austin*, and *Dahlstrom* establish, it is well within a legislature's power to protect individual privacy by limiting entities' ability to acquire sensitive information. Multiple courts, including the Illinois Supreme Court, have endorsed this approach to regulating individual data.

Clearview's logic would also imperil a number of similar Illinois statutes that limit the use of information pertaining to individuals. Illinois has enacted multiple laws, including the law criminalizing nonconsensual dissemination of private sexual images analyzed in *Austin*, that regulate information in a similar way to BIPA and thus would be unconstitutional under Clearview's reasoning. These include, amongst others, Illinois laws that regulate patient privacy and Social Security Numbers. 410 ILCS 50/3(d) ("Each physician, health care provider, health services corporation and insurance company shall refrain from disclosing the nature or details of services provided to patients…"); 5 ILCS 10(b) ("Except as otherwise provided in this Act, beginning July 1, 2010, no person or State or local government agency may do any of the

following: (1) Collect, use, or disclose a social security number from an individual…"). Because, as described *infra*, the Illinois legislature has made appropriate findings in these statutes and in BIPA that regulating the dissemination of information is necessary to further an important government interest, this Court should follow existing precedent and hold that BIPA does not impermissibly impinge Clearview's speech rights.

III. As a content-neutral time, place, and manner restriction, BIPA withstands intermediate scrutiny.

BIPA is content-neutral, as it does not discriminate against speech based on the content or ideas expressed, and therefore is subject to intermediate scrutiny.[2] Indeed, BIPA does not target content at all. Instead, as discussed *supra*, it regulates biometric identifiers, which are not speech. Any effects upon speech are purely incidental. Indeed, the regulation of the collection, use, and retention of biometric identifiers hardly constitutes the kind of impingement upon the marketplace of ideas that the First Amendment was designed to protect against.

In *Austin*, the Illinois Supreme Court identified a few major themes from the U.S. Supreme Court with regards to the intersection of privacy and speech, noting that "state laws protecting individual rights are long established and are not necessarily subordinate to First Amendment free speech protections" and that "the Court is wary of broad rules or categorical holdings framing the relationship between laws protecting individual privacy and the First Amendment." 2019 IL 123910 at *11. More specifically, in its analysis of the statute challenged in *Austin* the Illinois Supreme Court observed that, as a privacy law, it could be characterized as

[2] Courts have routinely applied intermediate scrutiny in upholding privacy statutes that impose consent requirements similar to BIPA's. *See, e.g.*, Trans Union Corp. v. F.T.C., 245 F.3d 809, 819 (D.C. Cir. 2001) (subjecting Fair Credit Reporting Act's ban of sale of target marketing lists to intermediate scrutiny); Boelter v. Hearst Communications, Inc., 192 F. Supp. 3d 427, 445 (S.D.N.Y. 2016) (subjecting Michigan's Video Rental Privacy Act's ban on nonconsensual disclosure of identifying information to intermediate scrutiny); Am. Civil Liberties Union of Illinois v. Alvarez, 679 F.3d 583, 608 (7th Cir. 2012) (concluding that the Illinois Eavesdropping Act's prohibition of recording even *public* conversations sweeps too broadly to withstand intermediate scrutiny).

a valid time, place, and manner restriction that satisfied the intermediate scrutiny standard. *Id.* at 10–16. This court should similarly construe BIPA as imposing a modest time, place, and manner restriction on expression by requiring consent for the acquisition and use of biometric identifiers and information.

Content-neutral time, place, and manner restrictions are subject to intermediate scrutiny, and under that standard "must be narrowly tailored to serve the government's legitimate, content-neutral interests but... need not be the least restrictive or least intrusive means of doing so." *Ward v. Rock Against Racism,* 491 U.S. 781, 798 (1988). BIPA easily passes this test.

Illinois has an important, legitimate interest in protecting individual privacy and, specifically, biometric identifiers. In enacting BIPA, the General Assembly specifically found that biometrics are "biologically unique" to individuals and therefore that biometric privacy has especially high stakes. 740 ILCS 14/5(c). In an era of increased reliance on biometric identifiers, the General Assembly found, additional regulation was necessary to reassure a public wary of its use. 740 ILCS 14/5(d)–(g).

Events since BIPA was enacted in 2008 underscore the General Assembly's concerns. Biometric identifiers can identify individuals, potentially without their knowledge, through analysis of images, video, and other visual media. Crucially, BIPA regulates the analysis of those media and the creation and use of biometric identifiers, rather than regulating the underlying media itself. The possible misuse of biometric information, without consent, has been the subject of much scholarly attention and reporting. *See* Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. Times (June 24, 2020) (describing how a facial recognition algorithm incorrectly identified a man as a suspect in a shoplifting case). Illinois' important interest in creating a framework governing such information — similar to its statutes regulating medical

privacy and Social Security Numbers — follows from the permanence of biometric information and the potential misuses of such information. 740 ILCS 14/5. Indeed, BIPA now seems remarkably prescient given that it predated the existence of Clearview AI and other companies that traffic in facial recognition software.

BIPA is narrowly tailored to achieve Illinois' interest in protecting privacy. Notably, BIPA does not *prohibit* biometric identifiers, but rather creates a consent-based framework for their collection and use. 740 ILCS 14/15. In using a consent-based framework that allows entities to create and manipulate biometric identifiers subject to collection, use, retention, and security conditions, BIPA creates a comprehensive regime to regulate information to individuals. This mirrors other privacy regulations, including those that have withstood First Amendment challenges such as the Fair Credit Reporting Act. *TransUnion v. FTC*, 245 F.3d 809 (D.C. Cir. 2001); *King v. Gen. Info. Sys.*, 903 F.Supp.2d 303 (E.D. Penn. 2012) (denying defendant's motion for judgment on the pleadings). By regulating, rather than prohibiting, the use of biometric identifiers and using long-head privacy principles to govern biometric information, the Illinois legislature properly tailored BIPA to promote individual privacy while minimizing any incidental effects on speech. As the Supreme Court recently noted in *McCutcheon v. Fed. Election Comm'n*, and the Illinois Supreme Court referenced in *Austin*, the fit need not be "perfect" but must merely be "reasonable." 572 U.S. 185, 218 (2014); 2019 IL 123910 at *10. BIPA meets this standard.

Because BIPA focuses on the regulation of biometric identifiers — a legitimate governmental interest — and is narrowly tailored, it easily meets the intermediate scrutiny standard that applies to content-neutral regulations.

CONCLUSION

For the foregoing reasons, *amici* urge the court to deny Clearview's motion to dismiss on First Amendment grounds. Clearview's erroneous arguments that BIPA violates the First Amendment contravene existing Illinois and federal law. Even if the court finds these arguments colorable, dismissing the case on First Amendment grounds at such an early stage of litigation — before the state has the opportunity to support the arguments that BIPA protects individual privacy as an important governmental interest — would not only destabilize the existing statutory regime protecting biometric information, but could also affect other Illinois privacy laws. We thus encourage the court to deny Clearview's motion to dismiss.

Date: November 2, 2020

Respectfully submitted:

/s/ Craig Futterman

Craig Futterman
MANDEL LEGAL AID CLINIC
UNIVERSITY OF CHICAGO LAW SCHOOL
6020 S. University Ave.
Chicago, IL 60637
(773) 702-9611
futterman@uchicago.edu
Cook County #91074

G.S. Hans*
STANTON FOUNDATION FIRST AMENDMENT CLINIC
VANDERBILT LAW SCHOOL
131 21st Ave. So.
Nashville, TN 37206
Tel.: (615) 343-2213
gautam.hans@vanderbilt.edu

** Application for admission pro hac vice forthcoming*

Counsel for amici Law Professors

APPENDIX (List of Signatories)[1]

Hannah Bloch-Wehba
Associate Professor of Law
Texas A&M University School of Law

Danielle Keats Citron
Austin B. Fletcher Professor of Law
Boston University School of Law

Julie E. Cohen
Mark Claster Mamolen Professor of Law and Technology
Georgetown University Law Center

Mary Anne Franks
Professor of Law and Dean's Distinguished Scholar
University of Miami School of Law

Woodrow Hartzog
Professor of Law and Computer Science
Northeastern University School of Law

Margot Kaminski
Associate Professor of Law
University of Colorado Law School

Genevieve Lakier
Assistant Professor of Law and Herbert and Marjorie Fried Teaching Scholar
University of Chicago Law School

Frank Pasquale
Professor of Law
Brooklyn Law School

Neil Richards
Koch Distinguished Professor in Law
Washington University in St. Louis School of Law

Scott Skinner-Thompson
Associate Professor of Law
University of Colorado Law School

[1] Amici's law school affiliations are stated for purposes of identification only. The views expressed herein represent the views of the individual signatories and should not be taken as the views of their universities.

CERTIFICATE OF SERVICE

The undersigned counsel certifies that on November 2, 2020, the foregoing was served on all counsel of record via email.

/s/ Craig Futterman
Craig Futterman