No. A167179

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA
FIRST APPELLATE DISTRICT
DIVISION 4

STEVEN RENDEROS, *ET AL.*,

Plaintiffs and Respondents,

v.

CLEARVIEW AI, INC.,

Defendant and Appellant.

APPLICATION TO FILE AND BRIEF OF *AMICI CURIAE* TECH JUSTICE LAW PROJECT, ELECTRONIC PRIVACY INFORMATION CENTER, AND CONSUMER FEDERATION OF AMERICA IN SUPPORT OF PLAINTIFFS-RESPONDENTS

Appeal from an Order of the Superior Court of California, Alameda County
The Honorable Judge Evelio Grillo
Case No. RG1096898

Meetali Jain (SBN 214237)
Melodi Dinçer (PHV Pending)
TECH JUSTICE LAW PROJECT
meetali@techjusticelaw.org
611 Pennsylvania Avenue SE
#337
Washington, DC 20003
Telephone: (202) 780-5750

Counsel for *Amici Curiae* Tech Justice Law Project, Electronic Privacy Information Center, and Consumer Federation of America

TO BE FILED IN THE COURT OF APPEAL **APP-008**

COURT OF APPEAL FIRST **APPELLATE DISTRICT, DIVISION** 4

COURT OF APPEAL CASE NUMBER: A167179

SUPERIOR COURT CASE NUMBER: RG1096898

ATTORNEY OR PARTY WITHOUT ATTORNEY: STATE BAR NUMBER: 214237
NAME: Meetali Jain
FIRM NAME: Tech Justice Law Project
STREET ADDRESS: 611 Pennsylvania Ave SE
CITY: Washington STATE: DC ZIP CODE: 20009
TELEPHONE NO.: FAX NO.: N/A
E-MAIL ADDRESS: meetali@techjusticelaw.org
ATTORNEY FOR (*name*): Amici Curiae Tech Justice Law Project et al.

APPELLANT/ PETITIONER: Clearview AI, Inc.

RESPONDENT/ REAL PARTY IN INTEREST: Steven Renderos et al.

CERTIFICATE OF INTERESTED ENTITIES OR PERSONS

(Check one): ☒ INITIAL CERTIFICATE ☐ SUPPLEMENTAL CERTIFICATE

Notice: Please read rules 8.208 and 8.488 before completing this form. You may use this form for the initial certificate in an appeal when you file your brief or a prebriefing motion, application, or opposition to such a motion or application in the Court of Appeal, and when you file a petition for an extraordinary writ. You may also use this form as a supplemental certificate when you learn of changed or additional information that must be disclosed.

1. This form is being submitted on behalf of the following party *(name*): Amici Curiae Tech Justice Law Project et al.

2. a. ☒ There are no interested entities or persons that must be listed in this certificate under rule 8.208.

b. ☐ Interested entities or persons required to be listed under rule 8.208 are as follows:

	Full name of interested entity or person	**Nature of interest *(Explain):***
(1)		
(2)		
(3)		
(4)		
(5)		

☐ Continued on attachment 2.

The undersigned certifies that the above-listed persons or entities (corporations, partnerships, firms, or any other association, but not including government entities or their agencies) have either (1) an ownership interest of 10 percent or more in the party if it is an entity; or (2) a financial or other interest in the outcome of the proceeding that the justices should consider in determining whether to disqualify themselves, as defined in rule 8.208(e)(2).

Date: November 4, 2024

Meetali Jain
(TYPE OR PRINT NAME)

Meetali Jain
(SIGNATURE OF APPELLANT OR ATTORNEY)

APPLICATION TO FILE *AMICI CURIAE* BRIEF

Under California Rules of Court rule 8.200(c)(4), the Tech Justice Law Center, Electronic Privacy Information Center, and Consumer Federation of America request leave to file the attached *amici curiae* brief in support of Respondents Steven Renderos *et al.*[1] The brief will aid the Court in understanding the applicability of the public interest exception, Cal. Civ. Proc. Code § 425.17(b), to Appellant Clearview AI, Inc,'s Motion to Dismiss the case pursuant to California's anti-SLAPP law, Cal. Civ. Proc. Code § 425.16. The brief will also aid the Court in understanding the historic relevance of the common law right of publicity to this case and the substantive fit between the required elements and Clearview's conduct integrating Respondents' unique facial information in their commercial facial recognition product without consent.

The Tech Justice Law Project (TJLP) is a legal initiative of Campaign for Accountability, a 501(c)(3) nonpartisan, nonprofit organization that uses research, litigation, and public communications to expose misconduct and malfeasance in public life. TJLP works with a collective of legal experts, academics, policy advocates, digital rights organizations, and technologists to

[1] Under Cal. Rule of Court rule 8.200(c)(3), *amici* certify that no party or counsel for any party authored this brief, participated in its drafting, or made any monetary contributions intended to fund the preparation or submission of the brief. *Amici* certify that no other person or entity other than the *amici* and their counsel authored or made any monetary contribution intended to fund the preparation or submission of the brief.

ensure that legal and policy frameworks are responsive to emergent technologies and their societal effects. TJLP advocates for better, safer, and more accountable digital spaces by convening a broad range of legal and technical expertise in numerous areas, including biometric privacy and data-based consumer harms.

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC advocates for strong, enforceable digital rights through participation in judicial, legislative, and regulatory processes. EPIC filed an *amicus* brief in *Martinez v. ZoomInfo* (9th Cir. 2023), 82 F.4th 785, supporting the plaintiff's right to sue an online data aggregator for violating the common law tort of misappropriation and California's statutory right of publicity.

Consumer Federation of America (CFA) is a national association of over 250 nonprofit organizations that advances the consumer interest through research, advocacy, education, and service. CFA investigates consumer issues and publishes research that assists policymakers and individuals, and it advances pro-consumer legislation at the national and state levels. CFA has worked with and advocated to federal and state consumer protection agencies to provide research and perspective about the need to address data exploitation and algorithmic harm.

Together, *Amici* represent data privacy and consumer protection organizations with special expertise in the ways that automated systems, including facial recognition, can exploit consumer data and implicate longstanding privacy rights. They have participated in numerous legal, advocacy, and public policy efforts to preserve consumers' control over personal information in the digital age, challenging business practices that profit from the nonconsensual collection and use of consumer data. These organizations serve the public's interest in better understanding the role of consumer data in the digital ecosystem and how best to protect consumer rights from data-based exploitation.

CONCLUSION

Amici respectfully request that the Court grant the application to file this *amici curiae* brief.

Dated: November 4, 2024

Respectfully submitted,

/s/ Meetali Jain
Meetali Jain (SBN 214237)
Melodi Dinçer (PHV Pending)
TECH JUSTICE LAW PROJECT
meetali@techjusticelaw.org
611 Pennsylvania Avenue SE
#337
Washington, DC 20003
Telephone: (202) 780-5750

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Kashmir Hill, *Clearview AI Successfully Appeals $9 Million Fine in the U.K.*, N.Y. Times (Oct. 18, 2023) 47

Kashmir Hill, *Clearview AI Used Your Face. Now You May Get a Stake in the Company.*, N.Y. Times (June 13, 2024)....................33, 51

Kashmir Hill, *Clearview AI's Facial Recognition App Called Illegal in Canada*, N.Y. Times (Feb. 3, 2021).....................................46

Kashmir Hill, *The Secret Company That Might End Privacy as We Know It*, N.Y. Times (Jan. 18, 2020)..38

Katherine Tangalakis-Lippert, *Clearview AI Scraped 30 Billion Images from Facebook and Social Media Sites and Gave Them to Cops: It Puts Everyone In a 'Perpetual Police Line-Up,'* Bus. Insider (Apr. 2, 2023)..53

Khari Johnson, *These Wrongly Arrested Black Men Say a California Bill Would Let Police Misuse Face Recognition*, CalMatters (June 11, 2024)..41

Letter from Ryan Mellino & Benjamin Powell, Staff Att'ys., Consumer Watchdog, to Rob Bonta, Cal. Att'y Gen., & Ashkan Soltani, Exec. Dir., Cal. Priv. Prot. Agency (Nov. 28, 2023).............45

Lindsey Holden, *Divisions Grow Over Use of Facial Recognition in California*, Gov't Tech. (Apr. 18, 2023) 41

Luke Broadwater, *Senators Seek to Curb Facial Recognition at Airports, Citing Privacy Concerns*, N.Y. Times (May 7, 2024) 40

Madison Alder, *House Republicans Probe NIST on Facial Recognition for Federal Digital Identity Verification*, FedScoop (Oct. 11, 2024) 40

Matthew D. Bunker & Emily Erickson, *The Jurisprudence of Public Concern in Anti-SLAPP Law: Shifting Boundaries in State Statutory Protection of Free Expression*, 44 Hastings Comm. & Ent. L.J. 133, 135–137 (2022).....................................24, 27

Melodi Dinçer & Nicola Morrow, *Clearview AI Is Deploying a California Law Meant to Protect Activists from Bogus Lawsuits*, Tech Pol'y Press (Aug. 15, 2023) 25

Mike Corder, *Clearview AI Fined $33.7 Million by Dutch Data Protection Watchdog Over 'Illegal Database' of Faces*, Associated Press (Sept. 3, 2024)...47

Morgan Meaker, *Clearview Stole My Face and the EU Can't Do Anything About It*, Wired (Nov. 7, 2022) 47, 49

Natasha Lomas, *Italy Fines Clearview AI €20M and Orders Data Deleted*, TechCrunch (Mar. 9, 2022) 46

INTRODUCTION

In just two decades, the widespread adoption of digital technologies and internet-connected products has produced a glut of personal information online. Everyday consumers' profiles, photos, videos, comments, and online behavior, combined with the digitization of information like their phone numbers, addressees, social memberships, and workplace affiliations, have spawned entire industries of companies that take this trove of personal information, package it into data-based insights, and sell access to those insights with abandon. This parasitic practice largely operates without consumers' knowledge or consent, and the companies whose valuations depend on this constant access to consumer data are not incentivized to change this status quo due to a lack of comprehensive, prospective data protections. Even in California, a leader in data protection law and enforcement, regulators struggle to keep up with violators who benefit from a decade-long head start in mass-appropriating consumer data as a foundational business practice.

As these mass data-driven practices become more commonplace, however, consumers have taken action to assert their long-standing constitutional, statutory, and common law privacy rights through litigation. As a result, courts increasingly recognize technologies that collect and process personal information at scale implicate privacy rights affecting the public interest. California courts are uniquely positioned in this landscape both practically, as the geographic nerve center of the tech industry, and legally, with a century of experience adjudicating cases concerning the commercial exploitation of peoples' personal information—be it in the mass-data products of today or the mass-media products of yesterday.

Appellant Clearview AI is a not only a paradigmatic example of this trend, but it takes mass data exploitation one step further by creating new information about everyone captured within its proprietary database. Clearview's conduct is more egregious than companies that simply aggregate personal information in a profile as it also extracts peoples' unique facial structures and reifies them in a machine-readable form as necessary conditions for its product to work. Clearview scrapes online images containing peoples' faces at scale, gathers those images into a proprietary database, extracts feature-based information from those images, converts them into standardized strings of numbers called facial vectors, runs algorithms trained on those vectors to take new images and identify similar vectors within the database, and sells access to this process to government agencies, including law enforcement, through its commercial facial recognition platform.

Respondents are just a few of the millions of Californians whose faces power Clearview’s internal database and end-user product, but not a single person consented to such use of their sensitive biometric information. Over the past four years, Clearview has faced numerous lawsuits, enforcement actions, and broad public scrutiny concerning its extensive misappropriation of peoples’ facial information for private profit. The present case is one such lawsuit, brought by Californian activists and advocacy groups whose privacy rights are implicated by Clearview’s conduct.

To avoid legal responsibility for its business model, Clearview now seeks cover under California’s broad anti-SLAPP law. In a circular logic, Clearview believes it is protected by the same law designed to protect nonprofits and common citizens from companies with deep pockets suing them into silence over their harmful business practices. The trial court rejected Clearview’s misplaced argument, and Clearview now appeals.

The trial court correctly ruled that this is not a SLAPP case. Far from it, Respondents' action seeks to redress the mass privacy violations suffered by Californians because of Clearview's exploitation of their online images without consent. Clearview's anti-SLAPP motion also fails because this suit falls under the public interest exception, Cal. Civ. Proc. Code § 425.17(b). This case aligns directly with California's public policy goal of preserving control over personal information—including one's likeness—against Clearview's nonconsensual collection and use of Californians' facial information at scale. On appeal, *amici* urge this Court to apply the public interest exception and allow this case to proceed for the following reasons.

First, Respondents seek the same relief personally as they seek for the greater public, in kind and degree. Their primary remedial request is for the court to grant injunctive and equitable relief as necessary to protect themselves, and all Californians, from Clearview's exploitation of their facial information, including acquiring, storing, and selling their likenesses to others. Second, if successful, this action would help vindicate millions of Californians' privacy rights against Clearview's violations, strengthening their existing right to control the use of their likeness by another for profit. This is a historic and traditionally valued right in California, where courts are sensitive to the loss of autonomy that attends commercial exploitation of one's identity. Third, private enforcement of these rights through this case is necessary and disproportionately burdensome to Respondents. To date, no public entity in California has sought to enforce these rights against Clearview, despite a bevy of international enforcement actions brought by countries with laws akin to the landmark California Consumer Protection Act (CCPA).

By allowing this case to proceed under the public interest exception, this Court will provide Respondents the chance to assert their common law right of publicity (ROP) claims against Clearview. Alongside constitutional privacy protections, the ROP is particularly well-suited to address the harms suffered by Californians due to Clearview's commercial exploitation of their identities in its product. The ROP is historically associated with mass technologies enabling the seamless reproduction of a person's likeness, without their consent and for private gain. Clearview represents yet another iteration of such mass technology, this time reproducing millions of Californians' likenesses throughout the lifecycle of the facial recognition process. Clearview used their likenesses at various points in the process, appropriated this information to its commercial advantage, lacked consent from Respondents and countless others for this use, and injured them as a result. Clearview's conduct maps on to each of the ROP requirements neatly, since the ROP exists precisely to combat the kind of autonomy harm Clearview's product enacts each time a user runs a probe image through the system.

Amici urge this Court to uphold the lower court's denial of anti-SLAPP protections to Clearview's conduct as alleged in this case. Clearview must face the consequences of its mass commercial exploitation of Californians' likenesses, controverting California's public policy commitment to preserving autonomy over the use of ones' identity. The public interest exception applies to this case and provides an additional basis for affirmance.

ARGUMENT

I. Courts increasingly recognize technologies that collect and process personal information at scale implicate privacy rights affecting the public interest.

The exponential growth of personal information online has inspired numerous companies to spin out data-based products and platforms. Many are unaware of the sheer number of such products, let alone the vastness of the databases that power them. *See How Americans View Data Privacy*, Pew Res. Ctr (Oct. 18, 2023);[2] Fed. Trade Comm'n, *Data Brokers: A Call for Transparency and Accountability* iv (May 2014).[3] Typically, for a fee, these companies range from gathering various forms of data into individual-based profiles—where personal information is itself the product—to extracting useful insights from mass amounts of compiled data, including through pattern-recognition algorithms and other machine learning processes. Fed. Trade Comm'n, *supra*, at i–v.

As these business models spread, it is harder for them to evade regulatory and legal scrutiny. Californians have been particularly successful in establishing legislative restrictions on companies processing their data at scale. The California Legislature has enacted landmark legislation, including the

[2] https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/ (noting an increase in respondents who understand little to nothing about what companies are doing with their personal data from 59% in 2019 to 67% in 2023).

[3] https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf ("Data brokers do not obtain [consumer data] directly from consumers, and consumers are thus largely unaware that data brokers are collecting and using this information.").

California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act, enshrining data privacy rights for consumers and reflecting the public's unequivocal interest in protecting personal information online. Cal. Civ. Code § 1798.100–1798.199.100. *See also* Cal. Bus. & Prof. Code § 22584–22585 (codifying the Student Online Personal Information Protection Act). These efforts supplement prior laws protecting personal information and are intended "to further the constitutional right of privacy"—not cancel it out. Cal. Civ. Code § 1798.175.

These legislative efforts coincide with consumers bringing legal actions to redress violations of their data privacy by a variety of companies. Within the past decade, courts across California and the U.S. have become more familiar with these mass data-based services and the morass of privacy harms they pose to modern society. *See, e.g.*, *In re Netflix Privacy Litig.* (N.D. Cal. Mar. 18, 2013) 2013 WL 1120801; *In re Facebook, Inc. Internet Tracking Litig.* (9th Cir. 2020) 956 F.3d 589; *Callahan et al. v. Ancestry.com Inc. et al.* (N.D. Cal. Mar. 1, 2021, No. 20-cv-08437-LB) 2021 WL 783524; *Kolebuck-Utz et al. v. Whitepages Inc.* (Apr. 22, 2021, No: 2:21-cv-0053) 2021 WL 1575219; *In re Google RTB Consumer Privacy Litig.* (N.D. Cal. June 13, 2022, No. 21-cv-02155) 606

F.Supp.3d 935; *Fed. Trade Comm'n v. Ring LLC* (D.D.C. May 31, 2023, No. 1:23-cv-1549) 2023 WL 3807179; *Carter v. Vivendi Ticketing US LLC* (C.D. Cal. Oct. 30, 2023) 2023 WL 8153712; *Ramirez v. LexisNexis Risk Solutions* (N.D. Ill. Apr. 8, 2024, No. 1:22-cv-05384) 2024 WL 1521448; *Calhoun et al. v. Google, LLC* (9th Cir. 2024) 113 F.4th 1141; Compl., *Carrera et al. v. Whitepages Inc.* (Sept. 5, 2024, No: 2:24-cv-10408); *Brooks et al. v. Thomson Reuters Corp.* (N.D. Cal. Oct. 10, 2024, No. 3:21-cv-01418-EMC) 2021 WL 3621837. This is especially so for companies collecting, storing, and processing biometric and genetic data of individuals who have not consented to their inclusion in these sensitive databases, in violation of longstanding constitutional, statutory, and common law privacy rights. *See, e.g.*, *In re Facebook Biometric Info. Privacy Litig.* (N.D. Cal. Feb. 26, 2021, No. 3:15-cv-03747-JD) 522 F.Supp.3d 617 (facial recognition features allegedly violated Illinois Biometric Information Privacy Act [BIPA]); *Vance et al. v. Microsoft Corp.* (W.D. Wash. Mar. 15, 2021) 525 F.Supp.3d 1287 (same); *K.F.C. by & though Clark v. Snap, Inc.* (S.D. Ill. June 10, 2021, No. 3:21-CV-9-DWD), 2021 WL 2376359, *aff'd sub nom.* *K.F.C. v. Snap Inc.* (7th Cir. 2022) 29 F.4th 835 (same); *In re TikTok Inc. Consumer Priv. Litig.* (N.D. Ill. 2021) 565 F.Supp.3d

1076 (same); *In re Anthem, Inc. Data Breach Litig.* (N.D. Cal. 2018) 327 F.R.D. 299 (massive data breach of personal, health, and financial information); *In re Ambry Genetics Data Breach Litig.* (C.D. Cal. 2021) 567 F.Supp.3d 1130 (similar); *In re 23andMe, Inc. Customer Data Sec. Breach Litig.* (N.D. Cal. Sept. 12, 2024, No: 3:24-md-03098-EMC) 2024 WL 4203646 (similar); *Portillo et al. v. Nebula Genomics, Inc. et al.* (N.D. Ill. Oct. 10, 2024, No. 1:24-cv-09894) 2024 WL 4471818 (alleged violations of genetic privacy law). *See generally* Surveillance Tech. Oversight Project, *Biometric Information Privacy Act (BIPA) Litigation Tracker* (2022).[4]

California courts are uniquely familiar with mass data-based services that implicate these rights. *See* Off. Att'y Gen. Cal. Dep't Just., *Privacy Enforcement Actions* (2024).[5] As companies are increasingly hauled to court, they are taking advantage of California's broad anti-SLAPP law, intended to protect nonprofits and citizens from large corporations attempting to sue them into silence and financial ruin. Matthew D. Bunker & Emily Erickson, *The Jurisprudence of Public Concern in Anti-SLAPP Law: Shifting Boundaries in State Statutory Protection of Free Expression*, 44

[4] https://www.stopspying.org/bipa-litigation-tracker.

[5] https://oag.ca.gov/privacy/privacy-enforcement-actions.

Hastings Comm. & Ent. L.J. 133, 135–137 (2022); *see, e.g.*, *Callahan et al. v. Ancestry.com Inc. et al.*, *supra*. Key to their strategy is to shoehorn specific product decisions, like mass scraping facial images from the internet and building a proprietary database, into the statute's catch-all provision, which protects from legal action "any other conduct in furtherance of the exercise of the constitutional right of petition or . . . of free speech in connection with a public issue or an issue of public interest." Cal. Civ. Proc. Code § 425.16(e)(4).

This strategy subverts the purpose of the anti-SLAPP law to protect ordinary people from powerful corporate entities attempting to "punish[] [them] for their speech" through litigation, especially when that speech is critical of business choices affecting the public interest. *X Corp. v. Ctr for Countering Digital Hate, Inc. et al.* (N.D. Cal. Mar. 25, 2024, No. 3:23-cv-03836-CRB) 2024 WL 1246318. Through this legal jiujitsu, tech company-Goliaths turn the anti-SLAPP law on its head to squash citizen-Davids' legal actions early on, avoiding the specter of discovery over their business practices. Bunker & Erickson, *supra*, at 137; Melodi Dinçer & Nicola Morrow, *Clearview AI Is Deploying a California Law Meant to Protect Activists from Bogus Lawsuits*, Tech Pol'y

Press (Aug. 15, 2023).[6] In response, plaintiffs have had to articulate repeatedly that collecting, processing, and selling personal information of millions of unwitting people is not protected conduct, even under the broadest interpretations of the statute.

Courts increasingly reject anti-SLAPP protections for companies attempting to use the statute to skirt legal liability for their mass data privacy violations. Instead, they allow lawsuits vindicating consumers' privacy rights to proceed under the statute's public interest exemption, Cal. Civ. Proc. Code § 425.17(b), which exempts "any action brought solely in the public interest or on behalf of the general public" under certain conditions. The U.S. Court of Appeals for the Ninth Circuit recently considered two challenges to data-aggregating products that raised similar facts and found the exception applied. In both cases, a person discovered that a company was gathering, organizing, and selling information about her online, and her profile was but one of many profiles replete with similar amounts and kinds of personal data. *See Batis v. Dun & Bradstreet*

[6] https://www.techpolicy.press/clearview-ai-is-deploying-a-california-law-meant-to-protect-activists-from-bogus-lawsuits/.

Holdings, Inc. (9th Cir. 2024) 106 F.4th 932; *Martinez v. ZoomInfo Technologies, Inc.* (9th Cir. 2023) 82 F.4th 785, *reh'g en banc granted*, *vacated* 90 F.4th 1042 (9th Cir. 2024). The company defendants transformed their information into a product and then sold it without receiving the plaintiffs' prior consent and without compensating them for such use of their names, likenesses, and other information. In both cases, the companies sought cover under the anti-SLAPP statute, filing motions arguing that their conduct arose from protected activity. The trial courts denied their anti-SLAPP motions on the basis that the companies failed to meet their burden to show this conduct was protected. On appeal, the Ninth Circuit found that both cases came within the public interest exception—even though the plaintiffs did not raise it in the trial proceedings—and affirmed denials of the anti-SLAPP motions on that ground.

While not binding on this court, these cases are instructive here. *See Martinez*, *supra*, 82 F.4th at 791 (applying California Supreme Court precedents). The lower court correctly denied Clearview's anti-SLAPP motion, finding that the company's nonconsensual collection and use of biometric information for sale in a facial recognition product is not protected speech even under the statute's broad catch-all provision, Cal. Civ. Proc. Code § 425.16(e)(4). On appeal, this Court should affirm that decision. Not only does Clearview's tortious conduct fall outside of the anti-SLAPP statute's ambit, but this action also vindicates the privacy rights of Californians harmed as a result. Accordingly, this Court should apply the public interest exception to Respondents' action, allowing the case to proceed.

II. Far from constituting a SLAPP action, this case seeks to vindicate California's public policy goal of preserving control over personal information—including one's likeness—against Clearview's nonconsensual collection and use of Californians' facial information.

When California became one of the first states to enact an anti-SLAPP statute in 1992, the Legislature directed that the law be "construed broadly" to deter legal actions aimed at silencing political expression through costly litigation. Cal. Civ. Proc. Code § 425.16(a). Over time, however, defendants gradually expanded the realm of possible conduct that could receive anti-SLAPP protections far beyond the Legislature's initial ambit. Bunker & Erickson, *supra*, at 148–49. As the California Supreme Court observed, "virtually always, defendants succeed in drawing a line—however tenuous—connecting their speech to an abstract issue of public interest." *FilmOn.com, Inc. v. DoubleVerify, Inc.* (2019) 7 Cal.5th 133, 140.

Eventually, the Legislature intervened to limit this trend in which largely corporate defendants used the anti-SLAPP law to "chill[] through abuse of the judicial process" participation in public issues affecting their business models. Cal. Civ. Proc. Code § 425.17(a). In the decade following the statute's enactment, the Legislature found that there had been a "disturbing abuse" of the law by litigants using it to stifle the same rights of speech and petition the law was intended to protect. *Id.* In 2003, it amended the statute to include a public interest exception, based on its finding that "it is in the public interest to encourage continued participation in matters of public significance." *Id.* According to the amendment's sponsor, it was enacted in response to precisely the kind of dynamic at play in this case: because "the same types of business who used the SLAPP action were inappropriately using [anti-SLAPP motions] against their public-interest adversaries." *People ex rel. Strathmann v. Acacia Rsch. Corp.* (2012) 210 Cal.App.4th 487, 499.

The public interest exception, Cal. Civ. Proc. Code § 425.17(b), exempts "any action brought solely in the public interest or on behalf of the general public" under certain conditions. The exception's applicability to a particular case is a matter of law that courts "must consider" prior to engaging in an anti-SLAPP analysis. *Takhar v. People ex rel. Feather River Air Quality Mgmt. Dist.* (2018) 27 Cal.App.5th 15, 24; *see also Batis v. Dun & Bradstreet Holdings, Inc.*, *supra*, at 936 fn. 2 (rejecting defendant's argument that plaintiff waived application of the exception by failing to raise it in the trial court because its application is an issue of law that "primarily involves assessing the face of [plaintiff's] complaint" and other fully-briefed facts).

Here, Clearview attempts to sidestep this statutory limit by tenuously connecting its for-profit facial recognition product to an "abstract issue of public interest"—a general concern for police identifying individuals suspected of criminal activity. *FilmOn.com, Inc.*, *supra.* Far from serving any public interest, the company's invocation of the anti-SLAPP statute *undermines* the public interest by harming Respondents' privacy rights. Respondents' action was brought solely in the public interest and intersects squarely with California's public policy goals of preserving individuals' control over their personal information against yet another mass data-driven, for-profit product that trades in their identities. As the Legislature intended, the public interest exception applies here precisely to combat Clearview's "disturbing abuse" of the judicial process in this case.

A. Respondents do not seek relief greater or different than what they seek for the Californian public—enjoining Clearview's facial recognition product.

The public interest exception requires that the plaintiff seek the same relief sought for the public, both in degree and kind. Cal. Civ. Proc. Code § 425.17(b)(1). Respondents brought this case against Clearview because the continued use of its product in California compounds violations of their privacy rights and threatens Californians' ability to safely exercise their free speech rights. In seeking injunctive and equitable relief, Respondents seek relief proportionate to the risk Clearview's product poses to any politically active Californian.

That individual Respondents seek monetary damages and allege emotional harms does not make the exception inapplicable to this case. *See Batis*, *supra*, at 937 (rejecting Respondent's argument that emotional distress damages are highly individualized and thus too personal a form of relief under the exception). Here, Respondents seek "injunctive and equitable relief as is necessary to protect themselves and other Californian residents" on the same terms. (1 CT 36.) Indeed, the organizational plaintiffs can seek injunctive relief only. *See* Pl.'s-Resp'ts Answering Br. at 48 (citing cases). The focus of this action is not personal pecuniary gain but prohibiting Clearview from continuing to profit off its misappropriation of millions of Californians' biometric information in violation of their rights.

This is not a case where Respondents seek certain kinds of relief to advance their own organizational interests or provide some advantage for a particular Respondent. *See Club Members for an Honest Election v. Sierra Club* (2008) 45 Cal.4th 309. Nor is it a class action where certain plaintiffs seek damages for themselves but not for other class members. *See Thayer v. Kabateck Brown Kellner LLP* (2012) 207 Cal.App.4th 141, 157 *as modified* (June 22, 2012) ("It is clear that Thayer seeks relief much greater than the relief sought for the purported class."). This is a case brought by Californian activists and advocacy organizations on behalf of all Californians whose interests are directly threatened by Clearview's business model.

Respondents share the same concerns over Clearview's scraping of Californians' facial images, producing facial vectors from those images, storing those vectors in a massive database, and selling access to this information to law enforcement throughout the state. The downstream effect of this conduct is that Respondents, along with other Californians who are politically active, could be identified and targeted by Clearview's users for exercising their constitutional rights. Their legal argument, however, concerns Clearview's upstream conduct that makes this possible, specifically the company's nonconsensual misappropriation of their likenesses in a proprietary database. Respondents collectively assert the violation of their privacy rights, and they are equally entitled to any form of relief that may result. *See Batis*, *supra*, at 937 ("[Any plaintiff] will have the opportunity to establish entitlement to any forms of relief for which [the defendant] is held liable."). They seek to hold Clearview accountable for the same unlawful behavior that affects every Californian whose face built and sustains its multimillion-dollar product. *See* Kashmir Hill, *Clearview AI Used Your Face. Now You*

May Get a Stake in the Company., N.Y. Times (June 13, 2024) (noting company's valuation).[7]

B. If successful, Respondents' action would help enforce millions of Californians' privacy rights against Clearview's incursions, including control over one's likeness which is a traditionally valued right in this state.

The public interest exception also requires that the successful action would "enforce an important right affecting the public interest" and would "confer a significant benefit" on the public. Cal. Civ. Proc. Code § 425.17(b)(2). The ability to control one's personal information generally and the ability to control the use of one's likeness specifically are well-established public policy goals in California. These are important privacy rights which Clearview undermines through its nonconsensual mass-collection and use of Californians' biometric information. If successful, Respondents' action would confer significant benefits to the public by enjoining Clearview's tortious conduct. This would disincentivize others from following Clearview's example, preventing similar mass violations of Californians' privacy rights.

[7] https://www.nytimes.com/2024/06/13/business/clearview-ai-facial-recognition-settlement.html.

It would also reassure Californians that they will not be subjected to Clearview's rights-eroding product when they exercise their speech and assembly rights in the future.

Respondents' action intersects with California's public policy goals of protecting individuals' right to control the use of their personal information by others, especially in digital contexts. *Tourgeman v. Nelson & Kennard* (2014) 22 Cal.App.4th 1447, 1463 ("[Courts must] examin[e] [the] complaint to determine whether [the] lawsuit is of the kind that seeks to vindicate public policy goals."). Through statute, Californians have determined that these consumer protections are necessary to protect the public in a data-driven age. *See* Cal. Civ. Code § 1798.100–1798.199.100; *see also* Issie Lapowsky, *California Unanimously Passes Historic Privacy Bill*, Wired (June 28, 2018) (quoting Sen. Robert Hertzberg, "We in California are continuing to push the envelope on technology and privacy issues by enacting robust consumer protections").[8]

More recent regulatory developments like the CCPA dovetail the historic right of control Californian's have over the use of their persona by others through the right of publicity (ROP). At the

[8] https://www.wired.com/story/california-unanimously-passes-historic-privacy-bill/.

center of the entertainment industry, Californians have a century-long tradition of challenging novel media technologies that allow advertisers, filmmakers, print publishers, videogame developers, and other entities to mass-reproduce individuals' likenesses without their consent, for commercial gain. *See, e.g.*, *Melvin v. Reid* (1931) 112 Cal.App. 285 (movie biography); *James v. Screen Gems, Inc.* (1959) 174 Cal.App.2d 651 (television); *Fairfield v. Am. Photocopy Equip. Co.* (1955) 138 Cal.App.3d 82 (advertisement); *Stilson v. Reader's Dig. Ass'n, Inc.* (1972) 28 Cal.App.3d 270 (advertisement); *Eastwood v. Superior Court* (1983) 143 Cal.App.3d 409 (tabloid); *Wendt v. Host Intern'l* (9th Cir. 1997) 125 F.3d 806 (animatronic robots); *Stewart v. Rolling Stone LLC* (2010) 181 Cal.App.4th 664, *as modified on denial of reh'g* (Feb. 24, 2010) (magazine editorial); *No Doubt v. Activision Publ'g, Inc.* (2011), 192 Cal.App.4th 1018 (video game avatars); *In re NCAA Student-Athlete Name & Likeness Licensing Litig.* (9th Cir. 2013) 724 F.3d 1268 (same).

In California, this right is democratic: there is no requirement under either the statutory or common-law right that the individual must be a celebrity or publicly known for violations to be actionable. *See Stilson v. Reader's Dig. Ass'n. Inc.*, *supra*, at

272 (using names of specific "townsmen" in sweepstakes advertisement); *Fairfield v. Am. Photocopy Equip. Co.*, *supra*, at 85 (listing name of Los Angeles-area lawyer in advertisement for photocopy machine). There are also no requirements that the appropriated likeness must appear in an advertisement or promotion for a separate product; indeed, there are several cases where courts applied the right where the likeness was itself the product or was embedded in a product, giving it commercial value. *See Comedy III Prods. v. Saderup* (2011) 25 Cal.4th 387, 394–96; *Lugosi v. Universal Pictures* (1979) 25 Cal.3d 813, 823; *James v. Screen Gems, Inc.*, *supra*; *see also* Restatement (Third) of Unfair Competition § 47 (Am. L. Inst. 1995) ("The name, likeness, and other indicia of a person's identity are used [for commercial exploitation] if they are used . . . in connection with services rendered by the user."). *See also* Cal. Civ. Code § 3344(a) (providing statutory ROP protection covering use of likeness "in products").

This long tradition underscores the state's public policy goal of protecting Californians' control over their likenesses and its recognition of this right as an important one affecting the public interest. *See Batis*, *supra*, at 937. Alongside the historic common law ROP, the right has also been recognized by a democratic body, the California Legislature, and enshrined in statute. Cal. Civ. Code § 3344. This history alone is sufficient to meet the second requirement of the public interest exception. *Id.* Yet, Clearview boldly asserts that there is no important right affecting public interest at issue in this case because most people in the U.S. support police use of facial recognition, without citing to any support legislative or otherwise. Def.-App.'s Reply Br. at 56–57. This assertion is not only irrelevant to the legal inquiry which focuses on California's public policy goals, but it is also unfounded.

The widespread availability of corporate facial recognition systems generally, and their use by law enforcement officers specifically, are far from settled public issues. Notably, the 2019 Pew Research Center survey Clearview cites for the idea that most people support police use of facial recognition was conducted prior to the police killing of George Floyd in May 2020 and subsequent mass protests. Aaron Smith, *More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly*, Pew Res. Ctr (Sept. 5, 2019).[9] This survey was also conducted before the New

[9] https://www.pewresearch.org/internet/2022/03/17/public-more-likely-to-see-facial-recognition-use-by-police-as-good-rather-than-bad-for-society/.

York Times exposé that brought Clearview's facial recognition product to public attention. Kashmir Hill, *The Secret Company That Might End Privacy as We Know It*, N.Y. Times (Jan. 18, 2020).[10] A more recent survey found that less than half of respondents thought widespread use of facial recognition technology by police is a "good idea for society," and almost a third believed it would be a "bad idea." *AI and Human Enhancement: Americans' Openness Is Tempered by a Range of Concerns*, Pew Res. Ctr (Mar. 17, 2022).[11] Those who were more familiar with the issue were much more likely to be in the latter camp. *Id.* This is significant, considering how law enforcement's lack of transparency about their reliance on facial recognition systems keeps the U.S. public largely in the dark. *Id.* The survey asked for respondents' views on police use of facial recognition generally but did not ask about police use of specific tools like Clearview's.

Beyond surveys, however, there are many other indicators that the negative impacts of facial recognition systems on privacy

[10] https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[11] Clearview also cites a survey commissioned by a tech industry think tank, NetChoice, that does not describe their methodology or provide sample survey questions.

rights is a live issue of public debate. Litigants recently settled a multidistrict litigation class action gathering several cases, all alleging Clearview violated privacy rights under various state and federal laws. Pl.'s Unopposed Mot. & Mem. in Supp. of Prelim. Approval of Class Action Settlement, *In re Clearview AI, Inc. Consumer Priv. Litig.* (N.D. Ill. June 12, 2024, No. 1:21-cv-00135).[12] Several states, cities, and localities across the U.S. have banned police use of facial recognition systems. *See* Fight for the Future, *Ban Facial Recognition: Interactive Map* (2022).[13] Federal consumer protection agencies have pursued large-scale enforcement actions against private facial recognition systems deployed against consumers. *See* Press Release, Fed. Trade Comm'n, *Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Reasonable Safeguards* (Dec. 19, 2023).[14] Federal lawmakers across political parties have questioned and challenged government use of facial

[12] Available: https://fingfx.thomsonreuters.com/gfx/legaldocs/znvnxzakbvl/Clearview%20Proposed%20Settlement.pdf.

[13] https://www.banfacialrecognition.com/map/ (last visited Oct. 26, 2024).

[14] https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without.

recognition, and state lawmakers in California have grappled with limiting police use of facial recognition as recently as this year. *See* Facial Recognition and Biometric Technology Moratorium Act, S. 681, 118th Cong. (2023);[15] Ethical Use of Facial Recognition Act, S. 3284, 116th Cong. (2020);[16] National Biometric Information Privacy Act, S. 4400, 116th Cong. (2020);[17] Fourth Amendment is Not For Sale Act, S. 1265, 117th Cong. (2021);[18] U.S. Comm'n C.R., *The Civil Rights Implications of the Federal Use of Facial Recognition Technology* (2024);[19] Alfred Ng, *Washington Takes Aim at Facial Recognition*, Politico (Jan. 19, 2024);[20] Luke Broadwater, *Senators Seek to Curb Facial Recognition at Airports, Citing Privacy Concerns*, N.Y. Times (May 7, 2024);[21] Madison Alder, *House Republicans Probe NIST on Facial Recognition for Federal Digital Identity Verification*, FedScoop (Oct. 11, 2024);[22]

[15] https://www.congress.gov/bill/118th-congress/senate-bill/681.

[16] https://www.congress.gov/bill/116th-congress/senate-bill/3284.

[17] https://www.congress.gov/bill/116th-congress/senate-bill/4400.

[18] https://www.congress.gov/bill/118th-congress/house-bill/4639.

[19] https://www.usccr.gov/files/2024-09/civil-rights-implications-of-frt_0.pdf.

[20] https://www.politico.com/news/2024/01/19/washington-takes-aim-at-facial-recognition-00136498.

[21] https://www.nytimes.com/2024/05/07/us/politics/airport-facial-recognition-technology-congress.html.

[22] https://fedscoop.com/house-republicans-probe-nist-on-facial-recognition-for-federal-digital-identity-verification/.

Lindsey Holden, *Divisions Grow Over Use of Facial Recognition in California*, Gov't Tech. (Apr. 18, 2023);[23] Khari Johnson, *These Wrongly Arrested Black Men Say a California Bill Would Let Police Misuse Face Recognition*, CalMatters (June 11, 2024).[24]

Clearview assumes that because many of their customers happen to be law enforcement agencies, the only public interest at issue here is whether police should be able to identify suspects of criminal activity. Far from engaging in criminal activity, however, individuals have been subjected to targeting by these systems for simply showing up to participate in large protests and express their constitutionally protected free speech rights. *See* Chris Morris, *Why Facial Recognition Technology Makes These Campus Protests Different from Those in the Past*, Fast Co. (May 2, 2024);[25] Alex Rozier, *Facial Recognition Tech Likely to Be Used to Identify Attackers at UCLA, Ex-LAPD Captain Says*, NBC L.A. (May 7, 2024);[26] *Inside the NYPD's Surveillance Machines*, Amnesty Int'l

[23] https://www.govtech.com/policy/divisions-grow-over-use-of-facial-recognition-in-california.

[24] https://calmatters.org/economy/technology/2024/06/face-recognition-technology-california/.

[25] https://www.fastcompany.com/91116791/facial-recognition-technology-campus-protests-police-surveillance-gaza.

[26] https://www.nbclosangeles.com/news/local/facial-recognition-tech-ucla-protest-attack/3407071/.

(2022);[27] James Vincent, *NYPD Used Facial Recognition to Track Down Black Lives Matter Activist*, Verge (Aug. 18, 2020);[28] United Nations Off. High Comm'r Hum. Rts., *Practical Toolkit for Law Enforcement Official to Promote and Protect Human Rights in the Context of Peaceful Protests* (2024).[29] As facial recognition systems become commonplace, public debate over their impacts on civil rights and liberties races further away from the neat resolution Clearview projects.

Whether or not the public generally supports widespread police use of facial recognition systems, this technology implicates the rights of millions of Californians where a private company, like Clearview, collects their facial images and uses them to power its product, without consent. This commercial exploitation of their likenesses intersects directly with California's historic public policy concern over preserving the public's right to control the use of one's likeness and protect it from misappropriation by corporate

[27] https://banthescan.amnesty.org/decode/index.html (detailing facial recognition surveillance of Black Lives Matter protestors by NYPD).

[28] https://www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram.

[29] https://www.ohchr.org/en/documents/tools-and-resources/practical-toolkit-law-enforcement-officials-promote-and-protect-human.

actors. Respondents' action seeks to enforce this important right affecting the public interest in the absence of enforcement action by California public authorities, including the California Privacy Protection Agency or Attorney General, against Clearview's unlawful conduct.

C. Private enforcement is both necessary and disproportionately burdensome as no public entity in the state has sought to enforce Californians' privacy rights against Clearview to date.

The final requirement of the public interest exception is that private enforcement is necessary and disproportionately burdensome on the plaintiffs. Cal. Civ. Proc. Code § 425.17(b)(3). While Californians have enshrined various data protections in law, no regulatory framework is static. Private enforcements of consumer data protections critically give meaning to regulatory efforts by allowing courts to interpret them in ways that respond directly to technologies as they evolve. This is especially so in the absence of direct public enforcement of Californians' robust privacy rights against companies whose business decisions undermine those protections.

This litigation is necessary to vindicate millions of Californians' rights because no public entity in the state has yet sought to enforce them against Clearview. The lack of public enforcement on its own makes private enforcement necessary. *See Batis*, *supra*, at 938 ("[t]his fact alone is a sufficient basis to conclude the action is 'necessary,' within the meaning of the public interest exception") (quoting *Inland Oversight Comm. v. Cnty. of San Bernadino* (2015) 239 Cal.App.4th 671, 676).

Clearview misinterprets this requirement in its briefing, ignoring the lack of public enforcement to argue instead that Respondents can simply opt-out of Clearview's database. Def.-App.'s Reply Br. at 58. Putting aside the unsubstantiated claim that exercising opt-out rights under the CCPA removes a person's facial information from Clearview's grasp, this is not how courts assess this requirement under California caselaw. Instead, the law is clear that, if there is no public enforcement of the same rights at issue in the action, then private enforcement is necessary—without more.

Despite calls to investigate the company for its unlawful business practices, Californian authorities have yet to act. *See* Letter from Ryan Mellino & Benjamin Powell, Staff Att'ys., Consumer Watchdog, to Rob Bonta, Cal. Att'y Gen., & Ashkan

Soltani, Exec. Dir., Cal. Priv. Prot. Agency (Nov. 28, 2023).[30] This is not the case elsewhere, however. Domestically, the Vermont Attorney General has pursued legal action against Clearview on behalf of its citizens' privacy rights. *Vermont v. Clearview AI, Inc.* (Vt. Sup. Ct. Dec. 18, 2023, No. 226-3-20-Cncv).[31] Internationally, several privacy regulators have determined that the same conduct challenged in this case violates the rights of the billions of individuals whose images were scraped and processed by Clearview, including Canada's privacy commissioner, Australia's Information/Privacy Commissioner, the United Kingdom's Information Commissioner's Office, France's Data Protection Authority, Italy's Data Protection Authority, Greece's Data Protection Authority, and most recently the Dutch Data Protection Authority. Off. Priv. Comm'r Can., *Clearview AI Ordered to*

[30] https://consumerwatchdog.org/wp-content/uploads/2023/12/Clearview-AI-Cover-Letter-and-Report.pdf.

[31] https://aboutblaw.com/bbZV. Notably in that case, the court denied Clearview's motion to dismiss because it failed to convince the judge that it had a First Amendment right to engage in facial recognition surveillance. *Vermont v. Clearview AI, Inc.* (Vt. Sup. Ct. Sept. 10, 2020, No. 226-3-20-Cncv), https://ago.vermont.gov/sites/ago/files/wp-content/uploads/2020/09/Clearview-Motion-to-Dismiss-Decision.pdf.

Comply with Recommendations to Stop Collecting, Sharing Images (Dec. 14, 2021);[32] Kashmir Hill, *Clearview AI's Facial Recognition App Called Illegal in Canada*, N.Y. Times (Feb. 3, 2021) (quoting Canada's privacy commissioner stating, "[w]hat Clearview does is mass surveillance, and it is illegal") (internal quotation marks omitted);[33] Off. Austl. Info. Comm'r, *Clearview AI Breached Australians' Privacy* (Nov. 3, 2021);[34] James Vincent, *Clearview AI Ordered to Delete Facial Recognition Data Belonging to UK Residents*, Verge (May 23, 2022);[35] Natasha Lomas, *France Latest to Slap Clearview AI with Order to Delete Data*, TechCrunch (Dec. 16, 2021);[36] Natasha Lomas, *Italy Fines Clearview AI €20M and Orders Data Deleted*, TechCrunch (Mar. 9, 2022);[37] *Hellenic DPA Fines Clearview AI 20 Million Euros*, Eur. Data Prot. Bd. (July 20,

[32] https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/an_211214/.
[33] https://www.nytimes.com/2021/02/03/technology/clearview-ai-illegal-canada.html.
[34] https://www.oaic.gov.au/newsroom/clearview-ai-breached-australians-privacy.
[35] https://www.theverge.com/2022/5/23/23137603/clearview-ai-ordered-delete-data-uk-residentsico-fine.
[36] https://techcrunch.com/2021/12/16/clearview-gdpr-breaches-france/.
[37] https://techcrunch.com/2022/03/09/clearview-italy-gdpr/.

2022);[38] Mike Corder, *Clearview AI Fined $33.7 Million by Dutch Data Protection Watchdog Over 'Illegal Database' of Faces*, Associated Press (Sept. 3, 2024).[39] These actions total $110 million in fines which Clearview has largely ignored. Adrianne Appel, *Clearview AI's GDPR Fines Rise to $110M Total After Latest Penalty by Dutch DPA*, Compliance Wk. (Sept. 9, 2024).[40] *See also* Morgan Meaker, *Clearview Stole My Face and the EU Can't Do Anything About It*, Wired (Nov. 7, 2022) ("Frustration is growing in Europe that face search engines [including Clearview AI] keep operating in blatant defiance of regulators' orders to stop processing EU faces");[41] Kashmir Hill, *Clearview AI Successfully Appeals $9 Million Fine in the U.K.*, N.Y. Times (Oct. 18, 2023) (noting that these fines may pose an existential threat to the company by exceeding its valuation).[42] In a joint statement, a

[38] https:// edpb.europa.eu/news/national-news/2022/hellenic-dpa-fines-clearview-ai-20-million-euros_en.

[39] https://apnews.com/article/clearview-ai-facial-recognition-privacy-fine-netherlands-a1ac33c15d561d37a923b6c382f48ab4.

[40] https://www.complianceweek.com/regulatory-enforcement/clearview-ais-gdpr-fines-rise-to-110m-total-after-latest-penalty-by-dutch-dpa/35338.article.

[41] https://www.wired.com/story/clearview-face-search-engine-gdpr/.

[42] https://www.nytimes.com/2023/10/18/technology/clearview-ai-privacy-fine-britain.html.

group of international privacy authorities reiterated that personal information that is "publicly accessible" online is "still subject to data protection and privacy laws in most jurisdictions." Int'l Enf't Coop. Working Grp., Glob. Priv. Assembly, *Joint Statement on Data Scraping and the Protection of Privacy* (2023).[43]

These public enforcement actions attempt to vindicate the rights of Canadians, Australians, UK citizens, Europeans, and even Vermonters—while Californians are left to fight Clearview through private enforcement, like this one, due to a lack of action by state authorities. Despite Clearview's likely violations of the CCPA,[44] including failing to provide adequate notice and receive consent prior to scraping Californians' facial images, being technically unable to permanently delete information for individuals who opt out under the law, and ignoring the law's special protections for collection and processing of facial images of

[43] https://ico.org.uk/media/about-the-ico/documents/4026232/joint-statement-data-scraping-202308.pdf.

[44] Clearview repeatedly claims it complies with the CCPA without providing any evidence and argues that its alleged compliance cancels out this legal action. The CCPA closely follows the European GDPR, including its notice and consent requirements, which several enforcing agencies have found Clearview violated in scraping images from social media and other websites without user knowledge or consent.

people under the age of sixteen, neither the CPPA nor the Attorney General has pursued action against the company to date. *See* Meaker, *supra*;[45] Ryan Mellino, Consumer Watchdog, *Regulators Should Use Existing Legal Tools to Rein in Clearview AI's Abuses of Our Personal Privacy Rights* 15–17 (2023).[46] Public enforcement is required under the CCPA in this case, which does not involve a data breach. *See* Cal. Civ. Code § 1798.150(b) (providing private right of action solely in response to security breaches of personal information); § 1798.199.90(a) (requiring civil actions to be brought by Attorney General).

Additionally, this lawsuit is currently one of the only avenues available for Californians to obtain injunctive relief against Clearview. *See In re Clearview AI, Inc. Consumer Priv. Litig.*, *supra* (providing no injunctive relief and only a potential for

[45] https://www.wired.com/story/clearview-face-search-engine-gdpr/ ("Clearview did not reply to a request to comment on whether it is able to permanently delete people from its database"); *id.* ("[an IT researcher] does not believe it's technically possible for Clearview to permanently delete a face [because] Clearview's technology, which is constantly crawling the internet for faces, would simply find and catalog him all over again.").

[46] https://consumerwatchdog.org/wp-content/uploads/2023/12/Clearview-AI-Cover-Letter-and-Report.pdf.

future monetary recovery to all class members, including Californians). Underscoring the public interest being served here, Respondents primarily seek injunctive and equitable relief. Personal compensation is not the main remedy Respondents seek. In fact, it is highly unlikely that the individual plaintiffs here are likely to recover significant financial awards, and even less likely that any damages will compensate them beyond the time and risk they have already invested in the case, which exposes them to potential attorneys' fees. *Cf.* Cal Jeffrey, *Clearview AI Wants to Pay Americans Pennies in Company Equity for Violating their Privacy*, TechSpot (June 14, 2024) (estimating the recent Clearview MDL settlement will provide class plaintiffs with just 30 cents each of equity in the company).[47]

Respondents' motivation in bringing and adjudicating this action is solely to ensure that Californians' rights are protected against Clearview's incursions through injunctive and equitable relief. Their desired remedy is to regain control over their identities in the face of Clearview's mass appropriations. They seek an outcome of this action that vindicates the rights of all

[47] https://www.techspot.com/news/103404-clearview-ai-wants-pay-americans-pennies-company-equity.html.

Californians, including themselves, whose images Clearview collected and continues to use to power its product unlawfully. *See* Hill, *Clearview AI Your Face. Now You May Get a Stake in the Company*, *supra*.[48]

III. Alongside constitutional privacy protections, the right of publicity uniquely addresses the harms suffered by Californians whose identities Clearview commercially exploited.

California's state constitutional right to privacy is historically tied to the use of personal information without consent. *See Batis*, *supra*, at 937–38 (discussing this connection and citing *Melvin v. Reid* (1931) 112 Cal.App. 285, 290). California courts have considerable experience deciding cases of commercial exploitation of identities, recognizing that it is "one of the most flagrant and common means of invasion of privacy." *Fairfield v. Am. Photocopy Equip. Co.*, *supra*, at 86. For over a century, the right of publicity (ROP) has evolved alongside mass-technological innovations enabling companies to exploit peoples' identities as

[48] https://www.nytimes.com/2024/06/13/business/clearview-ai-facial-recognition-settlement.html (quoting one privacy advocate, "[i]f mass surveillance is harmful, the remedy should be stopping [Clearview] from doing that, not paying pennies to the people who are harmed.").

part of their products: from portrait photography to mass-produced advertisements, magazine subscriptions to online databases, the right has preserved autonomy over how one's unique identity is used and perceived by others. This was especially so where new technologies captured a person's appearance and could seamlessly reproduce it without the subject's awareness, driving a new sense of entitlement and ownership over one's personal images later enshrined in the ROP. *See* Amici Curiae Br. Sci., Legal, & Tech. Scholars, *Renderos et al. v. Clearview AI Inc., et al.* (Sup. Ct. Cty Alameda, Sept. 19, 2022, No: RG21096898, at 3–5) (discussing historical co-development of the ROP with technologies based on mass-production of personal images). These historic instances of ordinary peoples' "physiognom[ies] . . . pirated to tout another person's business" mirror Clearview's modern piracy of billions of peoples' facial images to construct and maintain its for-profit facial recognition product. Samantha Barbas, *Laws of Image: Privacy and Publicity in America* 56 (2015).

The ROP is a particularly well-suited and well-developed privacy right to address the harms suffered by the millions of Californians whose faces drive Clearview's profits. Clearview trades in identity. It harvests the facial information of anyone who has ever appeared in an image online, with practically no way for a person to avoid being captured by Clearview’s automated web scrapers except to never appear in a single photo that could be uploaded to the internet. *See* Katherine Tangalakis-Lippert, *Clearview AI Scraped 30 Billion Images from Facebook and Social Media Sites and Gave Them to Cops: It Puts Everyone In a ‘Perpetual Police Line-Up,’* Bus. Insider (Apr. 2, 2023) (“[I]f you are in the background of a wedding photo, or a friend of yours posts a picture of you together at high school, once Clearview has snapped a picture of your face, it will create a permanent biometric print . . . in the database.”).[49] In addition to unjustly enriching Clearview, the company’s ongoing commercial exploitation of peoples’ facial information undermines their right to decide whether their identities should be used to build a mass surveillance technology, one to which many object. *See* Section II.C, *supra.* This strikes at the heart of the ROP, which preserves control over the use of a person’s identity from commercial exploitation, especially by purveyors of mass technologies like Clearview.

[49] https://www.businessinsider.com/clearview-scraped-30-billion-images-facebook-police-facial-recogntion-database-2023-4.

In this case, Respondents' ROP claim is consistent with those upheld by California courts for over a century. Respondents easily demonstrate the four elements of an ROP claim: (1) Clearview used their images or identities; (2) Clearview appropriated this information to the company's advantage; (3) neither Respondents nor millions of Californians consented to Clearview's use; and (4) they were injured as a result. *Stewart v. Rolling Stone LLC*, *supra*, at 679 (quoting *Eastwood v. Superior Court*, *supra*, at 416).

First, Clearview uses the actual images of individuals, their likenesses, and their identities throughout its facial recognition process. In building its product, Clearview first scraped billions of images of peoples' faces from the internet without their consent, a clear and intentional use of those images. *See Fleet v. CBS, Inc.* (1996) 50 Cal.App.4th 1911, 1918 (citing Restatement (Third) of Unfair Competition § 46 (Am. L. Inst. 1995). *See also White v. Samsung Elecs. Am., Inc.* (9th Cir. 1997) 971 F.2d 1395, 1398 ("[use] does not require that appropriations of identity be accomplished through particular means to be actionable."). The basis of Clearview's product and its richest resource is its massive database of facial information built from these scraped images. In this context, size matters. Clearview recognizes that the bigger its database, the better market advantage it has “in training an accurate algorithm.” Drew Harwell, *Facial Recognition Firm Clearview AI Tells Investors It’s Seeking Massive Expansion Beyond Law Enforcement*, Wash. Post (Feb. 16, 2022).[50] Next, Clearview uses these scraped images to train its algorithm with the unique facial vectors drawn from them. More images mean more facial vectors in its system, which translates to more data to calibrate the algorithm’s accuracy with each “successful” match of a probe image to an existing identity in the database. The result is the person’s identity—that is the point of the product. Clearview’s uses of identity are not only the intended outcome of its product, but also its main selling point.

Second, Clearview appropriates both the images of peoples’ faces within its database and their identities by constructing facial vectors that can uniquely identify a particular person. The ROP allows broad liability for the appropriation of *any characteristic* that has a clearly recognizable association with someone. *See, e.g.*,

[50] https://www.washingtonpost.com/technology/2022/02/16/clearview - expansion-facial-recognition/.

Zacchini v. Scripps-Howard Broadcasting Co. (1977) 433 U.S. 562 (unauthorized television broadcast of plaintiff's unique human-cannonball performance); *In re NCAA Student-Athlete Name & Likeness Litig.*, *supra* (unauthorized use of college football players' traits in video game avatars); *Brophy v. Almanzar* (C.D. Cal. Aug. 22, 2019, No. SAC 17-01885-8 CJC(JPRx)) 2019 WL 10837404 (unauthorized display of plaintiff's "unique and recognizable" back tattoo). Clearview's system mathematically constructs facial vectors drawn in part from certain measurements of facial features appearing in facial images. In the same way that videogame developers use math-based computational methods to turn a specific musician into an avatar, Clearview turns information from peoples' unique facial features into a machine readable and sortable string of numbers to facilitate facial recognition results. See *No Doubt v. Activision Publ'g, Inc.*, *supra* (videogame avatars based on specific musicians' appearances).

Clearview's algorithms construct recognizable associations based on the facial vector of anyone in its vast database. For the product to have any value, these vectors must map onto peoples' unique identities accurately. More faces in the system mean more accuracy, more accuracy means more value to customers, and more customers mean more profit for Clearview. Thus, Clearview's entire business strategy rests on its ability to mass appropriate individuals' likenesses with precision, and those likenesses are the foundation of its multimillion-dollar valuation.

Third, Clearview did not receive the consent of any of the millions of individuals whose likenesses it appropriates in its product. Clearview does not try to argue otherwise, as it would be nearly impossible to do so convincingly. Consent cannot be implied from people uploading images to various social media websites and other platforms in accordance with those sites' terms of service where Clearview later scraped those images without seeking specific consent and in violation of those terms; in fact, several of these platforms sent Clearview cease-and-desist letters concerning this conduct. *See Google, YouTube, Venmo and LinkedIn Send Cease-and-Desist Letters to Facial Recognition App that Helps Law Enforcement*, CBS News (Feb. 5, 2020).[51] *See also* Mem. Op. and Order, *ACLU v. Clearview AI, Inc.*, (Ill. Cir. Ct. Cook Cty 2021, No. 20 CH 4353, at *11) ("We must distinguish between the publicly-available photos Clearview harvested and what Clearview does

[51] https://www.cbsnews.com/news/clearview-ai-google-youtube-send-cease-anddesist-letter-to-facial-recognition-app/.

with them.”). By statute, California recognizes that “publicly available” information does not stretch far enough to include “biometric information collected by a business about a consumer without the consumer’s knowledge.” Cal. Civ. Code § 1798.140(v)(2) (defining “personal information” within the CCPA).

Clearview’s attempt to imply consent from a person’s failure to opt out of its database after the fact does not align with either the text of the CCPA as amended or how courts understand implied consent in ROP claims. *See* Cal. Civ. Code § 1798.140(h) (defining “consent” as “any freely given, specific, informed, and unambiguous indication of the consumer’s wishes . . . signif[ying] agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose.”); *No Doubt v. Activision Publ’g, Inc.*, *supra* (holding plaintiff band members’ consent to have look-a-like avatars play their songs in a video game did not establish consent to have those avatars play songs by other bands); *Greenley v. Kochava Inc.* (S.D. Cal. 2023) 684 F.Supp.3d 1024, 1039-1040 (rejecting data broker’s argument that failure to opt out implied consent where it did not disclose its data collection). Clearview all but admits its development of this product was nonconsensual when it recently launched a spin-off called, “Clearview Consent,” which it described as the company’s “First Consent Based Product.” *See* Clearview AI, *Clearview AI Launches Clearview Consent Company’s First Consent Based Product for Commercial Use* (May 25, 2022) (announcing the company’s “first consent based product” that is “separate and apart from the company’s database of 20+ billion facial images, the largest such database in the world.”).[52]

Finally, Respondents demonstrate injury on several levels because of Clearview’s commercial exploitation of their likenesses. There is direct injury in Clearview’s violation of their privacy rights, including their ROP. But there are also several associated injuries that flow from the violation of their rights. Respondents, like millions of Californians who learned about Clearview’s commercial exploitation of their identities after the fact, know that their online images undergird a powerful surveillance tool limited, by court order, to use by law enforcement and other government agencies. Several of these individuals are part of communities that are habitually targeted by these agencies based on their skin color,

[52] ttps://www.clearview.ai/clearview-ai-launches-clearview-consent-companys- first-consent-based-product-for-commercial-use.

ethnic identity, political beliefs, and/or religious affiliations. Even if Clearview's product is never used to directly identify them individually—something they may never know with certainty—it is regularly used by hundreds of government actors across the country to identify others, without regulatory limits on or transparency concerning this usage. Both the existence of Clearview's product and its widespread commercial success demonstrate how little control ordinary people have against technology companies who exploit their personal information for private gain. As this is the exact harm the ROP aims to address, Clearview's exploitative conduct in this case provides the Court with a simple application of law to facts.

Clearview demonstrates how easy it is for a tech startup to appropriate billions of peoples' images and identities without consent, enmesh those identities in its product, license that product widely, and reap the rewards. Clearview's continued licensing of this product and its use by several government actors demonstrates the urgent, overdue need for regulation and meaningful enforcement of existing privacy laws. The ROP provides a century-old avenue for relief in this dire landscape, and California courts historically apply it to rein in exploitative technologies that trade in personal identity. If the public interest exception applies to this case or, as the lower court found, Clearview cannot avail itself of anti-SLAPP protections, then it must face the consequences of its mass appropriation of Californians' likenesses. But even if anti-SLAPP applies, Respondents have demonstrated the merits of their ROP claim.

CONCLUSION

Amici respectfully request that this Court uphold the lower court's decision denying anti-SLAPP protection to Appellants.

Respectfully submitted,

/s/ Meetali Jain
Meetali Jain (SBN 214237)
Melodi Dinçer (PHV pending)
TECH JUSTICE LAW PROJECT
meetali@techjusticelaw.org
611 Pennsylvania Avenue SE
#337
Washington, DC 20003
Telephone: (202) 780-5750

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

Pursuant to California Rule of Court rules 8.204, in reliance on a word count by Microsoft Word, counsel for *amici* certify that the above brief is proportionately spaced, has a typeface of 13 points or more, and contains 10,585 words, inclusive of footnotes, which is within the 14,000-word limitation. The application and brief were prepared in 13-point Century Schoolbook font with 1.5 line spacing, 1-inch top and bottom margins, and 1.5-inch left and right margins.

Dated: November 4, 2024

Respectfully submitted,

/s/ Meetali Jain
Meetali Jain (SBN 214237)
Melodi Dinçer (PHV pending)
TECH JUSTICE LAW PROJECT
meetali@techjusticelaw.org
611 Pennsylvania Avenue SE
#337
Washington, DC 20003
Telephone: (202) 780-5750

Counsel for Amici Curiae

PROOF OF SERVICE

On November 4, 2024, I electronically served the document described below on the interested parties listed in the Service List that follows via TrueFiling on the TrueFiling website (tf3.truefiling.com) and/or by mail.

APPLICATION TO FILE AND BRIEF OF *AMICI CURIAE* TECH JUSTICE LAW PROJECT, ELECTRONIC PRIVACY INFORMATION CENTER, AND CONSUMER FEDERATION OF AMERICA IN SUPPORT OF PLAINTIFFS-RESPONDENTS

Dated: November 4, 2024

Respectfully submitted,

/s/ Meetali Jain
Meetali Jain (SBN 214237)
Melodi Dincer (PHV pending)
TECH JUSTICE LAW PROJECT
meetali@techjusticelaw.org
611 Pennsylvania Avenue SE
#337
Washington, DC 20003
Telephone: (202) 780-5750

Counsel for Amici Curiae

SERVICE LIST

Colin Vierra
EIMER STAHL LLP
1999 S. Bascon Ave.
Suite 1025
Campbell, CA 95008
cvierra@eimerstahl.com

Robert Edward Dunn
EIMER STAHL LLP
1999 S. Bascon Ave.
Suite 1025
Campbell, CA 95008
rdunn@eimerstahl.com

Jordan V. Hill
EIMSTAHL LLP
224 S. Michigan Ave., Suite 1100
Chicago, IL 60604
jhill@eimerstahl.com

Counsel for Defendant and Appellant Clearview AI, Inc.

First Appellate District, Fourth Division County of Alameda

By mail:
Clerk of the Superior Court of California, County of Alameda
Deliver to: Hon. Noël Wise
René C. Davidson Courthouse
1225 Fallon Street
Oakland, CA 94612

Sejal R. Zota
Just Futures Law
1629 K Street Suite #300
Washington, D.C. 20006
sejal@justfutureslaw.org

Dinesh K. McCoy
Just Futures Law
1629 K Street Suite #300
Washington, D.C. 20006
dinesh@justfutureslaw.org

Daniel J. Werner
Just Futures Law
1629 K Street Suite #300
Washington, D.C. 20006
daniel@justfutureslaw.org

Matthew Borden
BRAUNHAGEY & BORDEN LLP
351 California Street, Tenth Floor
San Francisco, CA 94104
borden@braunhagey.com

J. Noah Hagey
BRAUNHAGEY & BORDEN LLP
351 California Street, Tenth Floor
San Francisco, CA 94104
hagey@braunhagey.com

Counsel for Plaintiffs and Respondents Steven Renderos et al.