

No. A167179

**IN THE COURT OF APPEAL OF THE STATE OF
CALIFORNIA
FIRST APPELLATE DISTRICT, DIVISION FOUR**

STEVEN RENDEROS, *ET AL.*,

Plaintiffs and Respondents,

v.

CLEARVIEW AI, INC.,

Defendant and Appellant.

From the Superior Court of California for the County of Alameda
The Honorable Evelio Grillo, Judge Presiding
Case No. RG21096898

**BRIEF OF AMICUS CURIAE AMERICAN CIVIL
LIBERTIES UNION OF NORTHERN CALIFORNIA IN
SUPPORT OF PLAINTIFFS AND RESPONDENTS**

Nicolas Hidalgo (SBN 339177)
Nicole Ozer (SBN 228643)
Jacob Snow (SBN 270988)
ACLU Foundation of Northern
California
39 Drumm Street
San Francisco, CA 94111
(415) 621-2493
nhidalgo@aclunc.org
nozer@aclunc.org
jsnow@aclunc.org

Attorneys for Amicus Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES	3
INTRODUCTION	6
ARGUMENT	9
I. Clearview Cannot Justify Its Privacy Invasions.....	9
A. Clearview Has Engaged in Unlawful Privacy Invasions, Not First Amendment Activity Protected by California’s Anti-SLAPP Law	9
B. The CCPA Does Not—And Could Not—Displace the California Constitution	14
II. California Constitutional Privacy Rights Should Protect Against Clearview’s Actions	17
A. The California Constitutional Right to Privacy is Intended to Provide Robust Protections.....	17
B. Plaintiffs Have Committed Multiple Constitutional Privacy “Mischiefs”	21
C. Plaintiffs Have a Strong Constitutional Privacy Claim.....	30
1. Plaintiffs Have Legally Protected Privacy Interests	31
2. Plaintiffs Have a Reasonable Expectation of Privacy	34
3. Clearview Committed a Serious Invasion of Privacy	38
CONCLUSION.....	42
CERTIFICATE OF COMPLIANCE.....	43
PROOF OF SERVICE	44

TABLE OF AUTHORITIES

Cases	Page(s)
<i>ACA Connects - Am.'s Commc'ns Ass'n v. Frey</i> , 471 F. Supp. 3d 318 (D. Me. 2020)	12
<i>Am. Acad. of Pediatrics v. Lungren</i> , 16 Cal. 4th 307 (1997)	15
<i>Bartnicki v. Vopper</i> , 532 U.S. 514 (2001)	11, 13
<i>Bd. of Educ. v. Pico</i> , 457 U.S. 853 (1982)	13
<i>California Logistics, Inc. v. State of California</i> , 161 Cal. App. 4th 242 (2008)	14
<i>Carpenter v. United States</i> , 585 U.S. 296 (2018)	24
<i>City of San Diego v. Shapiro</i> , 228 Cal. App. 4th 756 (2014)	15
<i>Cnty. of Los Angeles v. Comm'n on State Mandates</i> , 150 Cal. App. 4th 898 (2007)	15
<i>Dye v. Council of City of Compton</i> , 80 Cal. App. 2d 486 (1947)	15
<i>Hill v. Nat'l Collegiate Athletic Ass'n.</i> , 7 Cal. 4th 1 (1994)	<i>passim</i>
<i>Ji v. Naver Corp.</i> , No. 21-cv-05143-HSG, 2022 WL 4624898 (N.D. Cal. Sep. 30, 2020)	32
<i>Katz v. United States</i> , 389 U.S. 347 (1967)	24
<i>Lamont v. Postmaster Gen. of U.S.</i> , 381 U.S. 301 (1965)	13

<i>NetChoice, LLC v. Bonta</i> , 113 F.4th 1101 (9th Cir. 2024)	11
<i>Patel v. Facebook, Inc.</i> , 932 F.3d 1264 (9th Cir. 2019)	32
<i>Sorrell v. IMS Health Inc.</i> , 564 U.S. 552 (2011)	24, 25
<i>Stand Up for California! v. State</i> , 64 Cal. App. 5th 197 (2021)	14
<i>White v. Davis</i> , 13 Cal. 3d 757 (1975).....	<i>passim</i>
<i>X Corp. v. Ctr. for Countering Digital Hate, Inc.</i> , No. 23-CV-03836-CRB, 2024 WL 1246318 (N.D. Cal. Mar. 25, 2024)	26
Statutes	
Cal. Civ. Code § 1798.175	16
Cal. Const. art. I, § 1	17, 20
Other Authorities	
<i>California Proposition 11, Constitutional Right to Privacy Amendment</i> , ballotpedia.org (1972)	17
<i>California Statewide Survey Re: Poll Results of Likely 2020 Voters</i> , David Binder Research.....	37
Becca Cramer-Mowder and Matt Cagle, <i>Once Again, California Refused to Endorse Face Surveillance. Now It's Time to Ban It</i> , Am. Civil Liberties Union of N. Cal. (Aug. 21, 2024)	36
Facial Recognition and Biometric Technology Moratorium Act, S. 681, 118th Cong. (introduced Mar. 7, 2023)	37
Kashmir Hill, <i>The Secretive Company That Might End Privacy as We Know It</i> , New York Times (Jan. 18, 2020)	36

Kashmir Hill and Ryan Mac, <i>‘Thousands of Dollars for Something I Didn’t Do,’</i> New York Times (Mar. 31, 2023)	29
Elizabeth Lopatto, <i>Clearview AI CEO Says ‘Over 2,400 Police Agencies’ Are Using Its Facial Recognition Software,</i> The Verge (Aug. 26, 2020).....	22
<i>NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software,</i> Nat. Inst. of Standards and Tech. (Dec. 19, 2019)	40
Nicole A. Ozer, <i>Golden State Sword: The History and Future of California’s Constitutional Right to Privacy to Defend and Promote Rights, Justice, and Democracy in the Modern Digital Age,</i> 39 Berkeley Tech. L.J. 963 (2024)	18, 32, 35
Nicole A. Ozer, Kate Ruane, and Matt Cagle, <i>Grassroots Activists are Leading the Fight to Stop Face Recognition. It’s Time for Congress to Step Up, Too,</i> Am. Civil Liberties Union (June 17, 2021)	37
<i>Right of Privacy California Proposition 11,</i> UC Law SF Scholarship Repository (1972)	12, 19, 24
<i>San Francisco Board of Supervisors Approves Historic Face Surveillance Ban and Oversight Law,</i> Am. Civil Liberties Union of N. Cal. (May 14, 2019)	36
Jacob Snow, <i>Amazon’s Face Recognition Falsely Matched 28 Members of Congress With Mugshots,</i> Am. Civil Liberties Union (July 26, 2018).....	40
Nathan Wessler and Kia Hamadanchy, <i>Letter Re Request for Comment on Civil Rights Implications of the Federal Use of Facial Recognition Technology</i> (April 8, 2024)	41
<i>Williams v. City of Detroit Case Page,</i> Am. Civil Liberties Union (Jan. 29, 2024)	40

INTRODUCTION

Clearview AI, Inc. (“Clearview”) violated Plaintiffs’ constitutional privacy rights by secretly harvesting billions of photographs and videos, using that personal information to generate faceprints of millions of Californians that captured immutable biometric information, building a massive database of this personal information, and then selling that biometric information for government surveillance.

This case concerns Clearview’s attempt to evade accountability for invading Plaintiffs’ privacy. The company’s primary contention on appeal is that its intrusive actions are First Amendment activity protected by California’s anti-SLAPP law. This argument makes a mockery of this important state anti-SLAPP law and what actually constitutes First Amendment protected activity. As Plaintiffs ably explain, the Superior Court correctly rejected this claim under the first step of the state anti-SLAPP analysis.¹ This Court should similarly reject this surveillance company’s attempt to skirt Plaintiffs’ claims and

¹ Plaintiff-Respondents’ Answering Brief at 12.

misuse this important state law that is intended to protect constitutional rights, not undermine them.

If the Court does reach the second step of the anti-SLAPP analysis, however, the American Civil Liberties Union of Northern California (“ACLU of Northern California”) urges careful consideration of the merits of Plaintiffs’ constitutional right to privacy claim. As explained in the application to file this amicus curiae brief, the ACLU of Northern California is deeply committed to protecting the California constitutional right to privacy and has decades of experience doing so. In this brief, we highlight two critical defects in Clearview’s arguments on the right to privacy.

First, Clearview attempts to distract the Court from the core constitutional privacy issues in this case by asserting that the California Consumer Privacy Act (“CCPA”)—a state *privacy* statute—somehow supplants the privacy protections of the California Constitution. This argument flies in the face of established doctrine of constitutional interpretation. The California Constitution is the supreme law of the state and cannot be supplanted by a state statute. The language of the

CCPA itself also makes clear that the statute was intended to harmonize with and supplement the right to privacy—not subvert it. The Court should reject Clearview’s argument.

Second, Clearview is wrong that Plaintiffs cannot demonstrate a reasonable probability of success on their California constitutional privacy claim. Indeed, while Plaintiffs only need to show that Clearview engaged in one cognizable privacy invasion, the company has engaged in numerous such invasions. Clearview violated Plaintiffs’ constitutional privacy rights when it secretly and non-consensually gathered Plaintiffs’ personal information and extracted their unique and immutable physical characteristics to build a massive face surveillance database for government customers.

Plaintiffs’ probability of success on their privacy claims is further buttressed by the important informational privacy and autonomy privacy interests implicated by Clearview’s face surveillance. Face surveillance invades privacy, undermines free expression and association, and is notoriously error-prone and biased. Plaintiffs have demonstrated a probability of success on their privacy claim.

This Court should therefore affirm the Superior Court's order denying Clearview's anti-SLAPP motion and reject its attempt to undermine Californians' fundamental privacy rights.

ARGUMENT

I. Clearview Cannot Justify Its Privacy Invasions

Clearview's attempt to defend its violation of Plaintiffs' constitutional right to privacy demonstrates a fundamental misunderstanding of California's anti-SLAPP law, constitutional supremacy, and the purpose and scope of the California constitutional right to privacy.

A. Clearview Has Engaged in Unlawful Privacy Invasions, Not First Amendment Activity Protected by California's Anti-SLAPP Law

The California anti-SLAPP law is an important state law that protects free speech rights and safeguards against frivolous lawsuits intended to intimidate people from speaking out on matters of public concern. Clearview's contorted reliance on the anti-SLAPP law subverts its purpose in order to evade accountability for its unlawful infringement on the core privacy interests of Californians. The Superior Court did not fall for Clearview's legal baloney and neither should this Court.

Plaintiffs are challenging intrusive business practices that are far afield from the activities protected by the anti-SLAPP law and the Superior Court correctly dismissed Clearview's arguments to the contrary. Clearview continues to make these anti-SLAPP arguments on appeal.² This Court should similarly reject these unsupported arguments.

The test for whether conduct is protected by the anti-SLAPP law is not synonymous with protection under the First Amendment, and this brief does not provide a technical analysis of the California anti-SLAPP statute or whether it is met here. Instead, we explain that even if the anti-SLAPP statute was not limited to the four specific categories described in Section 425.16(e), but instead applied to all First Amendment activity, Clearview still could not show that its conduct receives that protection.

Clearview claims essentially unlimited First Amendment rights to do whatever it wants with personal information of

² Appellant's Opening Brief at 25–41; Appellant's Reply Brief at 11–33.

Californians that it collected from the internet.³ This is not the law. The First Amendment is not a free pass to build surveillance technology for law enforcement that violates people’s rights. In fact, quite the contrary, the constitutional right to privacy complements, rather than conflicts with, the First Amendment.

Courts have long grappled with the interplay between privacy and free speech, and each of these constitutional rights must be taken into proper account. It is well-established that people have First Amendment rights to speak about a matter of public concern, even when that speech concerns information that was obtained in violation of a privacy law. *See Bartnicki v. Vopper*, 532 U.S. 514, 535 (2001). Further, laws that purport to protect privacy, but in fact trespass into content-based regulation of speech, improperly infringe on First Amendment rights. *See NetChoice, LLC v. Bonta*, 113 F.4th 1101, 1121 (9th Cir. 2024) (applying strict scrutiny to invalidate certain aspects of California’s Age-Appropriate Design Code Act). But many privacy laws are properly crafted, serve a sufficiently important

³ Appellant’s Reply Brief at 37–38.

government interest, and are thus not in conflict with the First Amendment. *See ACA Connects - Am.'s Commc'ns Ass'n v. Frey*, 471 F. Supp. 3d 318, 328 (D. Me. 2020) (denying trade association's motion for judgment on the pleadings based on First Amendment challenge to state online privacy statute).

Many privacy laws work in concert with free speech interests, including the California constitutional right to privacy. As the ballot measure for the California Privacy Amendment explained in 1972, “[t]he right of privacy is an important American heritage and essential to the fundamental rights guaranteed by the First, Third, Fourth, Fifth and Ninth Amendments to the U.S. Constitution. This right should be abridged only when there is compelling public need . . .”⁴

Strong privacy rights reinforce the ability to exercise First Amendment freedoms by creating spaces where people have the confidence to candidly communicate with friends and associates, seek out advice and community, indulge curiosity, and

⁴ *Right of Privacy California Proposition 11*, UC Law SF Scholarship Repository at 27 (1972), https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=1761&context=ca_ballot_props (last visited Oct. 27, 2024).

anonymously speak or access information. “Fear or suspicion that one’s speech is being monitored by a stranger . . . can have a seriously inhibiting effect upon the willingness to voice critical and constructive ideas.” *Bartnicki*, 532 U.S. at 533 (internal citations and quotations omitted). The U.S. Supreme Court has repeatedly held that the ability to receive information “is a necessary predicate to the recipient’s meaningful exercise of his own rights of speech, press, and political freedom.” *Bd. of Educ. v. Pico*, 457 U.S. 853, 867 (1982) (italics omitted). Privacy is key to ensuring that individuals feel free to exercise this First Amendment right to receive information. *Lamont v. Postmaster Gen. of U.S.*, 381 U.S. 301, 305–07 (1965). Without strong privacy protections—such as those in the California Constitution—people cannot fully exercise their First Amendment rights.

The Court should reject Clearview’s attempt to improperly use the California anti-SLAPP law to evade accountability for its invasions of privacy. It should also reject any attempt by Clearview to improperly use the First Amendment as a cudgel against California constitutional privacy rights that support the

free expression necessary for individuals and democracy to flourish.

B. The CCPA Does Not—And Could Not—Displace the California Constitution

Clearview argues that the California Consumer Privacy Act (“CCPA”) somehow displaces the inalienable privacy protections guaranteed by the California Constitution.⁵ This argument is wrong as a matter of both basic constitutional doctrine and the language of the CCPA itself.

First, constitutions are supreme to statutory law. This foundational precept of American law is also true of the California Constitution, which “is the fundamental and supreme law of this state as to all matters within its scope.” *Stand Up for California! v. State*, 64 Cal. App. 5th 197, 211 (2021) (internal citations and quotations omitted). Indeed, as “the supreme law of our state” the California Constitution is “subject only to the supremacy of the United States Constitution.” *California*

⁵ Appellant Opening Brief at 43–46 (“The California Consumer Privacy Act allows Clearview to gather, analyze, and sell biometric information.”); Appellant’s Reply Brief at 35–41 (same).

Logistics, Inc. v. State of California, 161 Cal. App. 4th 242, 250 (2008) (internal citations and quotations omitted).

Second, it is settled law in California that any conflict between a California statute and the Constitution should be resolved in favor of the Constitution. *E.g.*, *Dye v. Council of City of Compton*, 80 Cal. App. 2d 486, 490 (1947). California statutory law cannot replace or lower constitutional requirements, and examples abound, from election law,⁶ to tax law,⁷ and even privacy law itself.⁸ It is a feature of California’s democratic bedrock that “[a] statute cannot trump the Constitution.” *City of San Diego*, 228 Cal. App. 4th at 788 (citing *Cnty. of Los Angeles v. Comm’n on State Mandates*, 150 Cal. App. 4th 898, 904 (2007)).

⁶ *Dye*, 80 Cal. App. 2d at 489 (finding a statute that set out a procedure for ballot measure voting conflicted with the referendum powers in article IV, section 1).

⁷ *City of San Diego v. Shapiro*, 228 Cal. App. 4th 756, 784 (2014) (finding a special tax was invalid when it met a statutory standard but failed to meet the constitutional standard under article XIII A, section 4).

⁸ *Am. Acad. of Pediatrics v. Lungren*, 16 Cal. 4th 307, 348 (1997) (finding that a statute requiring minors to obtain parental or judicial consent before receiving an abortion infringed on article I, section 1’s right to privacy).

In other words, even if the CCPA conflicted with the constitutional right to privacy (it does not), the Court must interpret any conflicting provisions in favor of the Constitution.

Third, the language of the CCPA itself contradicts Clearview’s argument. The CCPA was passed to supplement—not supplant—existing privacy rights. The text of the statute itself says that the CCPA “is intended to ***further the constitutional right of privacy*** and to supplement existing laws relating to consumers’ personal information,” and that, “[w]herever possible, law relating to consumers’ personal information should be construed to harmonize with the provisions of this title.”⁹ The statute also clarifies that “in the event of a conflict between other laws and the provisions of [the CCPA], the provisions of the law that afford the ***greatest*** protection for the right of privacy for consumers shall control.”¹⁰ Wherever the CCPA could be interpreted to provide weaker privacy protections than the Constitution or other California laws, the text of the statute itself clarifies that the stronger privacy protections apply.

⁹ Cal. Civ. Code § 1798.175 (emphasis added).

¹⁰ *Id.* (emphasis added).

Clearview’s contortions of both constitutional and statutory law cannot excuse its violations of the constitutional right to privacy. Even if Clearview had complied with certain provisions of state privacy law (which it has not demonstrated), that makes no difference to the merits of this case. Clearview must also separately comply with the California Constitution.

II. California Constitutional Privacy Rights Should Protect Against Clearview’s Actions

Clearview’s surveillance practices are at the core of what the California constitutional privacy was designed to protect against. If the Court reaches the second prong of the anti-SLAPP analysis, it should find that Plaintiffs have shown a probability of prevailing on their constitutional claim.

A. The California Constitutional Right to Privacy is Intended to Provide Robust Protections

California voters enshrined an inalienable constitutional right to privacy in article I, section 1 of the California Constitution in 1972.¹¹ As originally intended, the provision

¹¹ 62.9% of voters supported Proposition 11. *California Proposition 11, Constitutional Right to Privacy Amendment*, ballotpedia.org (1972),

granted people the power to seek redress for privacy questions in the digital age by putting the burden on the alleged privacy invader to justify a privacy invasion with a compelling interest.¹²

The California constitutional right to privacy is a modern right to privacy, with its “moving force” a focused privacy concern “relating to the accelerating encroachment on personal freedom and security caused by increased surveillance and data collection activity in contemporary society.” *White v. Davis*, 13 Cal. 3d 757, 774 (1975). The ballot language for the constitutional right to privacy explained how the “proliferation of government snooping and data collecting is threatening to destroy our traditional freedoms.” *Id.* (citing ballot language). The ballot language further articulated that the Privacy Amendment’s purpose was to address the lack of “effective restraints on the information

[https://ballotpedia.org/California Proposition 11, Constitutional Right to Privacy Amendment \(1972\)](https://ballotpedia.org/California_Proposition_11,_Constitutional_Right_to_Privacy_Amendment_(1972)) (last visited Oct. 13, 2024).

¹² Nicole A. Ozer, *Golden State Sword: The History and Future of California’s Constitutional Right to Privacy to Defend and Promote Rights, Justice, and Democracy in the Modern Digital Age*, 39 Berkeley Tech. L.J. 963, 998–1000 (2024), [https://btlj.org/wp-content/uploads/2024/10/Ozer GoldenStateSword.pdf](https://btlj.org/wp-content/uploads/2024/10/Ozer_GoldenStateSword.pdf).

activities of government and business” and “create a legal and enforceable right of privacy for every Californian.” *Id.* (citing ballot language).

The California constitutional right to privacy is:

“the right to be left alone. It is a fundamental and compelling interest. It protects our homes, our families, our thoughts, our emotions, our expressions, our personalities, our freedom of communion, and our freedom to associate with the people we choose. It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us.”¹³

This constitutional right recognizes the importance of protecting against privacy intrusion by both the government and private parties,¹⁴ protecting both informational privacy and autonomy privacy interests, and the need to protect “personal information” in the modern digital world. *White*, 13 Cal. 3d at 774.

The California Supreme Court first interpreted the breadth of the constitutional right to privacy in *White v. Davis*. The

¹³ *Right of Privacy California Proposition 11* at 26-27.

¹⁴ “[A]rticle I, section 1 of the California Constitution creates a right of action against private as well as government entities.” *Hill v. Nat’l Collegiate Athletic Ass’n.*, 7 Cal. 4th 1, 20 (1994).

California Supreme Court identified some “principal mischiefs” at which the amendment is directed:

- (1) “government snooping” and the secret gathering of personal information;
- (2) the overbroad collection and retention of unnecessary personal information by government and business interests;
- (3) the improper use of information properly obtained for a specific purpose, for example, the use of it for another purpose or the disclosure of it to some third party; and
- (4) the lack of a reasonable check on the accuracy of existing records.

13 Cal. 3d at 775.

In *Hill v. National Collegiate Athletic Association*, the first California Supreme Court case to consider a privacy invasion by a private party, the Court confirmed that “the Privacy Initiative in article I, section 1 of the California Constitution creates a right of action against private as well as government entities.” 7 Cal. 4th at 20. But the majority decision in *Hill* added elements for plaintiffs to meet when bringing constitutional claims and crafted a new test for adjudicating privacy claims (hereinafter “*Hill* test”). Despite the additional burdens of the *Hill* test, Plaintiffs have shown a reasonable probability of success on the constitutional privacy claim and should obtain redress against

Clearview's invasions of both informational and autonomy interests.

B. Plaintiffs Have Committed Multiple Constitutional Privacy "Mischief"

Clearview's privacy invasions implicate multiple principal mischiefs at the core of the constitutional right to privacy, as identified by *White v. Davis*. Here, Clearview has engaged in (1) government snooping and the secret gathering of personal information; (2) overbroad collection and retention of unnecessary personal information by government and business interests; (3) the improper use of information properly obtained for a specific purpose, for example, the use of it for another purpose or the disclosure of it to some third party; and (4) the lack of a reasonable check on the accuracy of existing records.

(1) Clearview committed "*government snooping' and the secret gathering of personal information.*"¹⁵

There is little doubt that Clearview is in the business of exactly the type of government surveillance described by the first privacy mischief. Clearview's products are marketed specifically

¹⁵ *White*, 13 Cal. 3d at 775.

at law enforcement and the company is actually under a consent judgment that limits its ability to sell products to non-government clients.¹⁶ In Clearview’s own words, it provides “facial recognition technology to governmental and law enforcement agencies.”¹⁷ Clearview’s CEO has stated that in 2020, over 2,400 police agencies were using the company’s surveillance service.¹⁸ According to Clearview, its products allow law enforcement to identify virtually anyone simply by uploading a “probe’ photograph,”¹⁹ supercharging the ability of government agencies to track a person’s movements and activities. Clearview facilitates face surveillance and the government snooping it enables.

¹⁶ Plaintiff-Respondents’ Answering Brief at 17.

¹⁷ 3 C.T. 725; *see also* 2 C.T. 458 (Mulcaire Dep.); Appellant’s Opening Brief at 30 (Clearview claims its customers are “exclusively governmental entities . . . that are predominantly, if not exclusively, involved in law enforcement) (*citing* 1 C.T. 225).

¹⁸ Elizabeth Lopatto, *Clearview AI CEO Says ‘Over 2,400 Police Agencies’ Are Using Its Facial Recognition Software*, The Verge (Aug. 26, 2020)

<https://www.theverge.com/2020/8/26/21402978/clearview-ai-ceo-interview-2400-police-agencies-facial-recognition>

¹⁹ 1 C.T. 18; 2 C.T. 453 (Mulcaire Dep. 35:3-22).

Clearview also engages in the secret gathering of personal information. The Superior Court found that “Clearview collects the images and biometric information of California residents (including Plaintiffs) without notice or consent by scraping images from websites and platforms, such as Facebook, Twitter, and Venmo.”²⁰ Clearview hoovers up images of people without their consent, such as “images posted by friends or relatives and even images of people who inadvertently appear in the backgrounds of photographs taken by strangers.”²¹

Clearview attempts to justify its privacy-invasive actions by claiming that the case arises out of Clearview’s scraping²² of “publicly available” information.²³ But this argument misunderstands the history, purpose, and scope of the California constitutional right. The privacy right protects “personal information” broadly—“[f]undamental to our privacy is the ability

²⁰ 3 C.T. 725.

²¹ 1 C.T. 26 ¶ 31.

²² “Scraping” is the colloquial term for using automated processes to collect massive amounts of information from the internet.

²³ Appellant’s Opening Brief at 12.

to control circulation of personal information.”²⁴ Whether that personal information is “public” or “private” is not dispositive. Indeed, one of the primary concerns that the constitutional right to privacy addresses is the “improper use of information properly obtained for a specific purpose, for example, the use of it for another purpose or the disclosure of it to some third party.” *White*, 13 Cal. 3d at 775.

The U.S. Supreme Court has also recognized that a person “does not surrender all [privacy interests] by venturing into the public sphere,” but instead that “what one seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.” *Carpenter v. United States*, 585 U.S. 296, 310 (2018) (quoting *Katz v. United States*, 389 U.S. 347, 351–52 (1967) (cleaned up)). The Court also recognized that “[t]he capacity of technology to find and publish personal information, including records required by the government, presents serious and unresolved issues with respect to personal privacy and the dignity it seeks to secure.” *Sorrell v. IMS Health Inc.*, 564 U.S.

²⁴ *Right of Privacy California Proposition 11* at 27.

552, 579 (2011).²⁵ The so-called “publicly available” nature of a person’s information does not necessarily foreclose protection under the California constitutional right to privacy.

The Superior Court did not fully consider whether Clearview’s improper collection of personal information itself constituted a privacy invasion, cursorily reasoning that there was nothing unlawful about “scraping the internet . . .”²⁶ If this Court reaches the question, it should properly analyze the circumstances when personal information is collected and used for a purpose other than which it was initially shared—a core aspect of the privacy rights guaranteed to Californians.²⁷ By

²⁵ While the Court in *Sorrell* struck down the Vermont privacy law, the state law in that case restricted specific speakers and purposes while allowing the state to use the information freely. 564 U.S. at 580. The California constitutional right to privacy does not favor specific speakers or purposes, but applies broadly and equally against invasion by both government and private interests. *Hill*, 7 Cal. 4th at 20.

²⁶ 3 C.T. 726.

²⁷ While scraping could violate the purpose limitation principle of the constitutional privacy right, there are many circumstances where collecting information from the internet furthers a public purpose and is not at odds with the privacy right. The ACLU of Northern California has appeared in cases as amicus to support

secretly harvesting personal biometric information, analyzing it, and selling it to law enforcement for the purpose of mass face surveillance, Clearview has engaged in a principal privacy mischief of government snooping and the secret gathering of personal information.

(2) Clearview has committed “*overbroad collection and retention of unnecessary personal information by government and business interests.*”²⁸

Clearview has collected and retained billions of images and videos of millions of Californians.²⁹ Plaintiffs allege “Clearview has built the most dangerous facial recognition database in the nation by illicitly collecting over three billion photographs of unsuspecting individuals. Clearview’s database is almost seven

scraping in such circumstances. *E.g., X Corp. v. Ctr. for Countering Digital Hate, Inc.*, No. 23-CV-03836-CRB, 2024 WL 1246318, at *21 (N.D. Cal. Mar. 25, 2024) (“Researchers and Journalists Use Scraping to Enable Speech in the Public Interest and Hold Power to Account”) (*quoting* Brief of Amici Curiae ACLU *et al.*).

²⁸ *White*, 13 Cal. 3d at 775.

²⁹ Plaintiff-Respondent’s Brief at 15 (*citing* 1 C.T. 17; 2 C.T. 560).

times the size of the FBI's.”³⁰ The collection and retention of so many images and videos is unnecessary and overbroad on its own. But Clearview has gone even further by analyzing this personal information to distill and store information about people’s immutable biometric characteristics. Clearview uses the personal information it has collected and analyzes it using their algorithms to create a unique “faceprint” for each individual, which relies on a person’s immutable biological characteristics, such as “the position, size, and shape of the eyes, nose, cheekbones, and jaw.”³¹ Clearview has no legitimate interest for collecting this much information, distilling the images into intimate and personal biometric information, maintaining a massive database, and selling it to law enforcement.

The maintenance of so much unnecessary personal information also puts people at risk that their information could be subject to hacking or data breaches.³² By collecting and

³⁰ 1 C.T. 17 ¶ 2.

³¹ 1 C.T. 17 ¶ 4; *see also* 2 C.T. 452–454 (Mulcaire Dep. 33:24–35:22).

³² Clearview has a history of data breaches. 1 C.T. 29 ¶¶ 46–47.

maintaining this massive database of personal information, Clearview has engaged in another privacy invasion.

(3) Clearview has committed “*the improper use of information properly obtained for a specific purpose, for example, the use of it for another purpose or the disclosure of it to some third party.*”³³

Clearview’s scraping of Plaintiffs’ personal information was both secret gathering of personal information described in the first mischief, as well as a violation of the purpose limitation principle described in the third. The information that Clearview scraped from various websites, including social media platforms or professional networking sites, was not provided to Clearview for the purpose of fueling their face surveillance. Clearview never sought permission to use these images and videos, but instead just vacuumed them up without any regard to the original purpose for the information and why it was obtained.³⁴

Clearview’s clandestine harvesting of personal information from the internet and using it for a different purpose is the kind of

³³ *White*, 13 Cal. 3d at 775.

³⁴ 1 C.T. 26; 2 C.T. 452.

circumstance contemplated by this third type of privacy invasion and that the constitutional right to privacy was passed to address.

(4) Clearview “*lack[s] . . . a reasonable check on the accuracy of [its] existing records.*”³⁵

Clearview does not provide Californians the ability to check and correct existing records. While it claims to allow people to “opt-out,” Clearview’s general counsel confirmed that this opt-out system is ineffective, and Clearview continues to retain images even after receiving a deletion request.³⁶

Use of this inequitable surveillance technology invites unnecessary encounters with law enforcement, potential misidentifications,³⁷ and misinformed decisions about police use

³⁵ *White*, 13 Cal. 3d at 775.

³⁶ 2 C.T. 456 (Mulcaire Dep. 46:3-6, 46:12-18 (neither opt-out nor deletion mechanism removes a person’s photo from Clearview’s database)), 460–461 (Mulcaire Dep. 64:19-66:9 (there are no assurances Clearview will not use faceprints for training, even if a person submits an opt out or deletion request)).

³⁷ Kashmir Hill and Ryan Mac, ‘*Thousands of Dollars for Something I Didn’t Do,*’ *New York Times* (Mar. 31, 2023), <https://www.nytimes.com/2023/03/31/technology/facial-recognition-false-arrests.html>

of force. But even when a face surveillance algorithm is perfectly accurate, it is still vulnerable to other types of bias that pervade the databases and realities that underlie these systems. People suffer discrimination, bias, and risk of physical violence when their faceprints are captured by Clearview's surveillance database, and Clearview's failure to allow people to opt-out or correct their personal information is a lack of a reasonable check on the accuracy of existing records.

By misusing Plaintiffs' personal information to fuel face surveillance, Clearview has committed multiple privacy mischiefs that have been identified as core concerns of the California constitutional right to privacy.

C. Plaintiffs Have a Strong Constitutional Privacy Claim

To prevail on a constitutional privacy claim under the California Supreme Court's *Hill* test, plaintiffs must demonstrate: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy under the circumstances; and (3) conduct by the defendant that amounts to a serious invasion of the protected privacy interest. *Hill*, 7 Cal. 4th at 35-37. Once a plaintiff has satisfied the first three elements, the defendant can

argue, as an affirmative defense, that the invasion of privacy is justified because it substantially furthers one or more countervailing interests. *Id.* at 40. Plaintiffs should be able to satisfy the *Hill* test and have provided ample evidence in addition to their pleadings—including in the form of a thorough deposition of Clearview’s general counsel.³⁸ The Court should find they have shown a reasonable probability of success on their invasion of privacy claim.³⁹

1. *Plaintiffs Have Legally Protected Privacy Interests*

Hill requires plaintiffs to demonstrate a legally protected privacy interest. Here, going beyond the mischiefs discussed above, Plaintiffs can demonstrate this in spades.

Clearview’s privacy invasions implicate not only Californians’ informational privacy rights—the interest in precluding the dissemination or misuse of personal information—

³⁸ 2 C.T. 444–482 (Mulcaire Dep.).

³⁹ In overruling Clearview’s related demurrer, the Superior Court found Plaintiffs had adequately alleged “a legitimate privacy interest, a reasonable expectation of privacy, and an egregious breach of social norms.” 3 C.T. 731.

but also their autonomy privacy rights—the interest in making intimate personal decisions or conducting personal activities without observation, intrusion, or interference. *Hill*, 7 Cal. 4th at 35.⁴⁰

First, Clearview violated the informational privacy interests of the Plaintiffs by surreptitiously collecting their personal information and using it to distil even more intimate and immutable information in the form of unique biometric “faceprints.” Federal courts in California have recognized a “cognizable privacy interest in one’s facial biometric information, even in photos that have been uploaded to a photo-sharing site.” *Ji v. Naver Corp.*, No. 21-cv-05143-HSG, 2022 WL 4624898, *10 (N.D. Cal. Sep. 30, 2020) (*citing Patel v. Facebook, Inc.*, 932 F.3d 1264, 1267, 1275 (9th Cir. 2019)). That Clearview has engaged in multiple privacy mischiefs in its collection and use of people’s

⁴⁰ The right to privacy protects both informational and autonomy privacy. More than twenty years after the right was added to the State Constitution, in *Hill*, the majority decision promulgated different standards for adjudicating autonomy and informational privacy claims – a distinction not present in the language or legislative history of the privacy right. *See Ozer, Golden State Sword*, at 1006–1008.

biometric information further supports the argument that they have violated the informational privacy interests that people have in their own personal information.

Next, Clearview’s surveillance technology also violates people’s autonomy privacy interests because the biometric information collected, and the ways that it can be used, restrict people’s ability to conduct their lives with freedom and dignity. Clearview’s law enforcement clients can use its face surveillance “to identify people with dissident views, monitor their associations, and track their speech.”⁴¹

Law enforcement can take a photograph of a person at a political rally or place of worship, upload it to Clearview’s database and instantly review other photographs of the same person along with links to various social media platforms and websites, which often describe a person’s address, employment, political affiliations, religious activities, familiar and social relationships, and other sensitive information.⁴² This face surveillance system allows law enforcement to learn how and

⁴¹ 1 C.T. 17 ¶ 2.

⁴² 1 C.T. 18 ¶ 5.

where people practice their First Amendment freedoms of expression, speech, and worship, all without ever receiving consent, demonstrating probable cause, or obtaining a warrant. It can easily be used to target and identify individuals because they attended a political rally, visited an abortion clinic, or attended a religious service.

In sum, Clearview’s surveillance system violates peoples’ autonomy privacy by restricting their ability to make intimate personal decisions or conduct personal activities without observation, intrusion, or interference. Autonomy privacy interests may only be justified by a showing of a “compelling interest,” which Clearview cannot demonstrate here. *Hill*, 7 Cal. 4th at 35.

2. *Plaintiffs Have a Reasonable Expectation of Privacy*

Plaintiffs can meet the “reasonable expectation of privacy”⁴³ requirement by showing it was reasonable for people to

⁴³ *Hill* imported the “reasonable expectation of privacy” element into the adjudication of the California constitutional privacy right from Fourth Amendment jurisprudence. The reasonable expectation of privacy was not present in the legislative history of

expect that Clearview would not collect their immutable biometric information and misuse it to fuel face surveillance systems.

“A ‘reasonable’ expectation of privacy is an objective entitlement founded on broadly based and widely accepted community norms.” *Hill*, 7 Cal. 4th at 37. “[C]ustoms, practices, and physical settings surrounding particular activities may create or inhibit reasonable expectations of privacy.” *Id.* at 36. “A plaintiff’s expectation of privacy in a specific context must be objectively reasonable under the circumstances, especially in light of the competing social interests involved.” *Id.* at 26–27.

The Superior Court recognized that Clearview collected Plaintiffs’ images and biometric information “without notice or consent by scraping images from websites and platforms.”⁴⁴ Plaintiffs were never put on notice of Clearview’s scraping and

the California constitutional right to privacy. *Ozer, Golden State Sword*, at 1009.

⁴⁴ 3 C.T. 725.

Clearview kept its practices secret until exposed by the *New York Times*.⁴⁵

Californians should not be expected to tolerate the gathering or maintenance of their personal biometric information and its use for face surveillance. Californians have been at the forefront of pushing back against face surveillance. San Francisco passed the first prohibition on face surveillance in 2019⁴⁶ and diverse coalitions have successfully pushed back multiple times on state legislative efforts supported by law enforcement to greenlight use of this dangerous surveillance technology.⁴⁷

⁴⁵ Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, *New York Times* (Jan. 18, 2020), <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>

⁴⁶ *San Francisco Board of Supervisors Approves Historic Face Surveillance Ban and Oversight Law*, Am. Civil Liberties Union of N. Cal. (May 14, 2019), <https://www.aclunc.org/news/san-francisco-board-supervisors-approves-historic-face-surveillance-ban-and-oversight-law>

⁴⁷ Becca Cramer-Mowder and Matt Cagle, *Once Again, California Refused to Endorse Face Surveillance. Now It's Time to Ban It*, Am. Civil Liberties Union of N. Cal. (Aug. 21, 2024), <https://www.aclunc.org/blog/once-again-california-refused-endorse-face-surveillance-now-it-s-time-ban-it>

The vast majority of people in California do not want the government to be able to track them using biometric information like face surveillance. In a statewide poll of likely voters, 82% of people disagreed with the government being able to monitor and track a person using biometric information.⁴⁸ Opposition to face surveillance has continued to grow⁴⁹ and a federal moratorium on the use of face surveillance by law enforcement was reintroduced in early 2023.⁵⁰

There is strong support that people have a reasonable expectation that their personal information would not be

⁴⁸ *California Statewide Survey Re: Poll Results of Likely 2020 Voters*, David Binder Research, https://www.aclunc.org/docs/DBR_Polling_Data_On_Surveillance.pdf (last visited Nov. 1, 2024).

⁴⁹ Nicole A. Ozer, Kate Ruane, and Matt Cagle, *Grassroots Activists are Leading the Fight to Stop Face Recognition. It's Time for Congress to Step Up, Too*, Am. Civil Liberties Union (June 17, 2021), <https://www.aclu.org/news/privacy-technology/grassroots-activists-are-leading-the-fight-to-stop-face-recognition-its-time-for-congress-to-step-up-too>

⁵⁰ S. 681, the Facial Recognition and Biometric Technology Moratorium Act of 2023, was introduced in the Senate on March 7, 2023. [https://www.congress.gov/bill/118th-congress/senate-bill/681#:~:text=Introduced%20in%20Senate%20\(03%2F07%2F2023\)&text=This%20bill%20imposes%20limits%20on,state%2C%20and%20local%20government%20entities](https://www.congress.gov/bill/118th-congress/senate-bill/681#:~:text=Introduced%20in%20Senate%20(03%2F07%2F2023)&text=This%20bill%20imposes%20limits%20on,state%2C%20and%20local%20government%20entities)

misappropriated to create unique and immutable faceprints that can be used to surveil them.

Clearview's secrecy and the widespread opposition to face surveillance systems support Plaintiffs' argument that they have a reasonable expectation of privacy that their personal information would not be used to fuel face surveillance.

3. *Clearview Committed a Serious Invasion of Privacy*

Hill requires plaintiffs to show a "serious invasion" of privacy. 7 Cal. 4th at 6. An invasion of privacy must be sufficiently serious in its nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right. The extent and gravity of the invasion is an indispensable consideration in assessing an alleged invasion of privacy. *Id.* Plaintiffs can also meet this burden that Clearview's invasion of privacy is serious.

First, Plaintiffs argue that "Clearview extracts biometric information from Plaintiffs' immutable physical characteristics, such that once Clearview enters an individual into its database,

that individual permanently loses anonymity and privacy.”⁵¹ The biometric information Clearview scrapes is indeed immutable. No one expects that a casual photo of themselves posted on the internet will be analyzed to capture their immutable biometric information. By maintaining a database of sensitive biometric information, Clearview also puts people at risk of misuse and data breaches. Yet unlike a password or a credit card number, a person cannot reset his or her face if it is compromised due to a breach of a database.

Next, Plaintiffs argue that Clearview’s invasion is serious “because it places Plaintiffs’ and Plaintiffs’ members lives and livelihood in danger, both from being misidentified to law-enforcement and immigration agencies and from being correctly identified and targeted for retaliation for their public political stances.”⁵² Here, Plaintiffs address a very serious concern with face surveillance, especially when these systems are in the hands of law enforcement. Face surveillance technology poses grave civil rights concerns because it enables anyone who uses the

⁵¹ 1 C.T. 37 ¶ 87.

⁵² 1 C.T. 37 ¶ 87.

technology to automatically track people's identities, whereabouts, and associations. Some of this danger also comes from errors, and face surveillance is very error-prone.⁵³ Those errors can and have led to wrongful arrests. Such was the case for Robert Williams, a Black man who was wrongly identified by face surveillance and improperly arrested in front of his family. His lawsuit against the Detroit Police Department ended with a settlement putting safeguards in place to limit the department's use of face surveillance.⁵⁴ Notably, nearly every known wrongful

⁵³ *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, Nat. Inst. of Standards and Tech. (Dec. 19, 2019), [NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software | NIST](#); Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots*, Am. Civil Liberties Union (July 26, 2018), [Amazon's e Recognition Falsely Matched 28 Members of Congress With Mugshots | ACLU](#).

⁵⁴ *Williams v. City of Detroit Case Page*, Am. Civil Liberties Union (last updated Jan. 29, 2024), <https://www.aclu.org/cases/williams-v-city-of-detroit-face-recognition-false-arrest>

arrest due to police reliance on an incorrect face surveillance result has been a Black person.⁵⁵

Even when accurate, face surveillance systems such as Clearview’s allow the government to spy on our every move. Police using face surveillance can know who you are, where you go, what you do, and who you do it with—engaging in political activities, seeking medical care, attending religious services, and more.

Clearview’s face surveillance system poses all of these threats and more. Clearview’s creation, maintenance, and sale of a massive face surveillance database to law enforcement is a serious invasion of privacy and constitutes an egregious breach of the social norms underlying the privacy right.

Clearview violated Plaintiffs’ legally protected privacy rights, Plaintiffs have a reasonable expectation of privacy, and Clearview’s invasion was serious. Accordingly, if this Court reaches the merits question in this anti-SLAPP case, it should

⁵⁵ Nathan Wessler and Kia Hamadanchy, *Letter Re Request for Comment on Civil Rights Implications of the Federal Use of Facial Recognition Technology* at 4 (April 8, 2024), [ACLU-Comment-to-USCCR-re-FRT-4.8.2024.pdf](#).

hold that Plaintiffs have demonstrated a probability of success on their constitutional right to privacy claim.

CONCLUSION

Clearview's conduct was not protected speech, its CCPA argument is unsupported, and Plaintiffs have a strong constitutional privacy claim. The Court should affirm the Superior Court's denial of Clearview's anti-SLAPP motion.

Sincerely,

/s/ Nicolas Hidalgo

Nicolas Hidalgo (SBN
339177)

Nicole Ozer (SBN 228643)

Jacob Snow (SBN 270988)

ACLU Foundation of

Northern California

39 Drumm Street

San Francisco, CA 94111

(415) 621-2493

nhidalgo@aclunc.org

nozer@aclunc.org

jsnow@aclunc.org

CERTIFICATE OF COMPLIANCE

Pursuant to California Rule of the Court 8.204(c)(1), I certify that the text in the attached Amicus Brief was prepared in Microsoft Word, is proportionally spaced, and contains 6,227 words, including footnotes but not the caption, the table of contents, the table of authorities, signature blocks, or the application.

Dated: November 4, 2024

By: /s/ Nicolas Hidalgo

PROOF OF SERVICE

I, Sara Cooksey, declare that I am over the age of eighteen and not a party to the above action. My business address is 39 Drumm Street, San Francisco, CA 94111. My electronic service address is scooksey@aclunc.org. On November 4, 2024, I served the attached,

APPLICATION FOR LEAVE TO FILE BRIEF OF AMICUS CURIAE

BRIEF OF AMICUS CURIAE AMERICAN CIVIL LIBERTIES UNION OF NORTHERN CALIFORNIA IN SUPPORT OF PLAINTIFFS AND RESPONDENTS

BY E-MAIL OR ELECTRONIC TRANSMISSION: I caused to be transmitted to the following case participants a true electronic copy of the document via this Court's TrueFiling system:

Counsel for Plaintiffs/Respondents:

Sejal Zota
Daniel Werner
Dinesh McCoy
JUST FUTURES LAW
95 Washington St., Suite 104-149
Canton, MA 94111
(919) 698-5015
sejal@justfutureslaw.org
daniel@justfutureslaw.org
dinesh@justfutureslaw.org

Matthew Borden
J. Noah Hagey
Tracy Olivia Zinsou
Braun Hagey & Borden LLP
351 California Street, Tenth Floor
San Francisco, CA 94104
borden@braunhagey.com
hagey@braunhagey.com
zinsou@braunhagey.com

Counsel for Defendant/Appellant:

Robert Edward Dunn
Collin James Vierra
EIMER STAHL LLP
1999 S. Bascom Ave., Suite 1025
Campbell, CA 95008
rdunn@eimerstahl.com
cvierra@eimerstahl.com

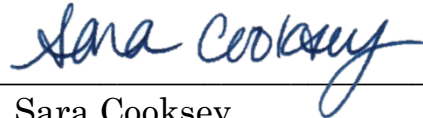
Jordan V. Hill
EIMER STAHL LLP
224 S. Michigan Ave., Suite 1100
Chicago, IL 60604
jhill@eimerstahl.com

BY MAIL: I mailed a copy of the document identified above by depositing the sealed envelope with the U.S. Postal Service, with the postage fully prepaid.

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

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Executed on November 4, 2024 in Fresno, CA.

A handwritten signature in blue ink that reads "Sara Cooksey". The signature is written in a cursive style and is positioned above a horizontal line.

Sara Cooksey
Declarant