Using Proposition 11 to revive California's privacy right in Renderos v. Clearview AI

Overview

Facial recognition technology and AI-driven surveillance raise urgent and pressing questions about privacy. One company in particular, Clearview AI, has created controversy over its surveillance technology. The company has been banned in Canada, sanctioned across Europe, and faced lawsuits challenging its practices in the United States. One such lawsuit, *Renderos v. Clearview AI*, is currently making its way through California courts. The case represents one of the first tests for courts to determine how modern AI surveillance interacts with California's once-strong privacy protections. As a matter of both law and public policy, the courts should take the opportunity to revive the state constitutional right to privacy by realigning with the original intent of 1972 Proposition 11 and finding this modern technology violates California's constitution.

Analysis

California's constitutional right to privacy, established by Proposition 11 in 1972, was intended to give individuals meaningful control over their personal information. Yet over time California courts have strayed from this purpose by erecting demanding thresholds for plaintiffs bringing privacy claims. As a result, privacy cases have largely failed in California courts, leaving the state's once-vigorous privacy protections ill-suited to address modern technology. *Renderos* raises the question of whether Proposition 11's promise is still a force in the age of facial recognition and biometric surveillance.

The path forward can be found by returning to first principles. The arguments favoring Proposition 11 centered on protecting Californians from rampant data collection, misuse, and surveillance. Early cases like *White v. Davis* and *Valley Bank v. Superior Court* reflected those principles, but later decisions such as *Hill v. NCAA*

narrowed the right and weakened its enforceability. The court's task in *Renderos* is to recognize that Clearview's practices implicate a protected privacy interest in biometric data, that individuals reasonably expect privacy in their information and movements, that the company's conduct is a serious invasion of that interest, and that any asserted justifications do not outweigh the harms. To realign the constitutional promise with today's technological threats, the court should look to Proposition 11's original intent as the guiding framework.

How *Renderos* intersects with California constitutional privacy

The 1972 ballot initiative was drafted in response to concerns about the unchecked growth of government surveillance, data misuse, and how advancing technology would lead to privacy intrusions.[1] The core message of the measure's arguments in favor was control: Californians should decide when and how their personal information is collected and used. Such control is essential to "social relationships and personal freedom," including the freedom to associate with whomever we want.[2] Most threatening to this freedom is the loss of control over the accuracy of information collected by the government and businesses.[3] Without control over the information gathered on us, we cannot correct the "inevitable mistakes" contained in the record. When it passed California became the first state to enshrine a privacy right in its constitution.

The momentum for individual privacy rights continued to build through the first two California Supreme Court cases to interpret the reach of the privacy amendment, *White* and *Valley Bank*. In *White*, the court held that the Los Angeles police department's surveillance practices infiltrating classes and student organization meetings at the University of California, Los Angeles were a prima facie violation of the constitutional right to privacy and could potentially chill protected First Amendment activity.[4] In *Valley Bank*, the court balanced discovery rights and customer privacy, finding the bank at issue was required to notify customers and provide them an opportunity to object before disclosing their confidential information.[5] These two decisions upheld the principal purpose of the constitutional right to privacy as giving Californians the ability to control the collection and

dissemination of their personal information.

Although the trajectory of privacy rights seemed promising following these cases and others in the two decades after the constitutional amendment, a turning point came with the California Supreme Court's 1994 decision in *Hill v. NCAA*. In *Hill*, the court ruled the NCAA's mandatory drug testing program for student-athletes did not violate their constitutional right to privacy.[6] In doing so, the court created a new three-part test: to bring a constitutional privacy claim, plaintiffs must show a recognized privacy interest, a reasonable expectation of privacy, and an invasion serious enough to "constitute an egregious breach of the social norms."[7] This framework raised the bar for plaintiffs and gave courts more leeway to justify intrusions by the government and private parties. *Hill* marked the moment California's privacy clause began to weaken.[8]

Enforcing the right to privacy has proved especially challenging as courts have been unable to evolve with advancing technology.[9] Plaintiffs often struggle to show that the behavior underlying invasion of privacy claims is serious enough, or that there is a reasonable expectation of privacy for online data, with 80% of constitutional privacy claims being rejected between 2009 and 2021.[10] Consequently, there is no clear path for plaintiffs to prove that new technologies like artificial intelligence surveillance and facial recognition surpass social norms to the level of serious privacy invasions. Although California courts have not yet analyzed how this technology interacts with the state constitutional right, federal courts in California have found that other online data practices such as accessing personal data collected and stored from a mobile phone app, tracking and transmitting historical vehicle performance and location, or collecting and disclosing to third parties unique device identifiers, personal data, and geographic information are not serious invasions under California's constitution.[11] Californians overwhelmingly voted to protect their privacy in 1972, but in the digital age, the gap between that constitutional promise and lived reality has widened.

The opportunity in *Renderos*

Renderos v. Clearview AI is the first real chance in decades for state courts to determine whether the constitutional right to privacy still has teeth. The case centers on Clearview AI's facial recognition app, built by scraping billions of images of people's faces from social media platforms without consent. Clearview claims a database of over 60 billion images, marketed to law enforcement for rapid identification of individuals. Critics warn the technology enables mass surveillance, eroding anonymity in public life. The company has faced global backlash, including sanctions in Europe, a ban in Canada, and restrictions in several U.S. states.[12]

In California, immigrant rights groups and political activists allege the technology violates their privacy, chills political speech, and disproportionately harms communities of color.[13] The complaint charges that the company uses AI technology to extract biometric information in scraped images, creating a "faceprint" by relying on immutable biological characteristics that "serves as a key for recognizing that individual in other images."[14] The complaint warns that Clearview's surveillance technology provides "instantaneous access to almost every aspect of our digital lives," and can be used to identify people shopping at the grocery store, attending political rallies, or simply walking down the street.[15] Plaintiffs included a constitutional claim of invasion of privacy: they claim that unauthorized access, use, and sale of biometric data infringes interests in controlling personal information and biometric identifiers.[16]

Clearview responded with an anti-SLAPP motion, arguing its collection and use of facial data is protected speech under the First Amendment. In a win for Californians, that argument failed because Clearview's commercial business supplying search results to law enforcement is not protected First Amendment activity contributing to public discourse.[17]

The appellate court's decision has two key implications. First, the court framed privacy rights and free speech as reinforcing, not undermining, each other. Had Clearview prevailed, California's anti-SLAPP statute would have insulated Clearview from liability for its alleged privacy invasions in the name of free speech, setting a precedent making it far more difficult to hold similar companies accountable and

effectively gutting constitutional privacy protections against modern surveillance. This was the right outcome, as the First Amendment was not intended to protect illegal activity undertaken in support of participation in public discourse.[18] If Clearview is violating California's constitutional right to privacy with its database, the First Amendment should not shield Clearview from liability for that invasion. And by rejecting Clearview's anti-SLAPP defense, the appellate court cleared the way for the trial court to address the core issue: whether facial recognition and AI surveillance represent serious invasions of privacy under the state constitution. The original intent of Proposition 11, as reflected in early cases like *White* and *Valley Bank*, was to ensure courts could adapt privacy protections to new technological threats. That intent should guide the court's analysis in *Renderos.*

A legally protected privacy interest

Clearview's harvesting of biometric data from social media websites implicates Proposition 11's concern with surreptitious surveillance and unnecessary data-gathering. Californians should have a legally protected interest in their facial biometric information embedded in photos uploaded to social media websites. Today, it is virtually impossible not to be captured online — intentionally or inadvertently — in our daily lives as images circulate across platforms. Clearview scrapes those images for biometric data and uses AI technology to create "faceprints" that link individuals to other photos in its database without people's consent. It then aggregates this information to build dossiers of people's daily activities.

The ballot arguments in 1972 warned of exactly that: the "accelerating encroachment on personal freedom and security caused by increased surveillance and data collection activity in contemporary society."[19] Clearview's technology realizes that fear because it enables government agencies and private actors alike to identify someone in public and instantly access other sensitive details about their work, political or religious affiliations, or health decisions.[20] Anyone with access to Clearview's database can weaponize the information for surveillance on people's movements and associations. The danger presented is not new. As the court recognized in *White*, surveillance that catalogues political activity or everyday

interactions poses an acute risk to First Amendment freedoms. If offline behavior can be captured, logged, and potentially monitored, people may alter the way they act in public and engage socially: avoiding protests, refraining from dissent, or otherwise curtailing constitutionally protected expression.[21]

Beyond chilling speech, Clearview's technology creates tangible risks of harm through misuse. For example, wrongful arrests based on misidentification from facial recognition technology are common and well-documented.[22] Recently, the Federal Trade Commission prohibited Rite Aid from using this technology for surveillance purposes after it failed to prevent harassment and false accusations stemming from its systems.[23] The risks extend beyond misidentification: biometric data can leave people exposed to stalking, harassment, spoofing, and identity theft.[24] Proposition 11 was intended to protect against these very types of threats of personal privacy and security by strengthening control over how personal information is collected, compiled, and disseminated.[25] Because biometric identifiers cannot be changed or concealed once exposed, Californians have a legitimate interest not only in avoiding misuse of such data but in safeguarding the ability to go about daily life free from constant observation. Clearview's technology compromises that protection, making the interest in biometric information both distinct and indispensable.

A reasonable expectation of privacy

Perhaps the most difficult element will be showing there is a reasonable expectation of privacy in biometric data extracted from online photos. "A 'reasonable' expectation of privacy is an objective entitlement founded on broadly based and widely accepted community norms."[26] Expectations about online privacy have shifted in the digital era, with many willing to accept less privacy in exchange for the free flow of information and social media connection. In fact, research shows that the vast majority of the American public believe they have little to no control over what companies do with their data online.[27] But concern over how businesses handle user data is growing, and in California, a statewide poll of likely voters confirmed that Californians don't want the government to be able to monitor and

track them using biometric data. As public pushback against biometric surveillance grows, community norms and expectations about privacy online will change. Policymakers have already signaled their intent to step in to fill the constitutional privacy gaps, but there must be corresponding judicial action.[28] In *Renderos*, grounding the reasonable expectation of privacy in contractual terms, user actions, and long-standing limits on surveillance ensures Proposition 11's core promise remains central.

Social media users can create a reasonable expectation by indicating an intent to maintain privacy by limiting access. Generally, signing up to share photos or information on a platform requires consent to the platform's terms of service, which sets the terms of access. Clearview's image scraping violates many such terms of service and abuses that expectation.[29] Uploading a photo, or appearing in someone else's photo, exceeds the scope of consent and should not mean consenting to its transformation into a biometric identifier that unlocks a permanent online dossier. By assenting to a platform's rules, users should reasonably expect that their data will only be used in accordance with those rules.[30] Users reinforce this expectation by activating privacy settings within social media websites or otherwise taking actions to maintain privacy, like un-tagging themselves in photos, turning off location sharing features, and changing default privacy settings. Yet one premise of Clearview's technology is it bypasses those precautions, and a user may still appear in Clearview's database if anything was ever shared publicly, with or without the user's consent.[31] Because these choices reflect a clear intent to set boundaries on how information circulates online, courts should treat them as supporting the reasonableness of an expectation of privacy — even if technology like Clearview's disregards them. The invasion itself should not dispel an expectation's reasonableness.

Beyond expectations tied to contractual and user choices, Clearview's retroactive surveillance capabilities implicate the expectation of privacy in the whole of an individual's physical movements.[32] Clearview indiscriminately captures and stores photos without any temporal limitation. This type of information gathering represents a shift in the control of our offline lives and how much of ourselves we

choose to reveal.[33] The information it aggregates and stores facilitates retroactive surveillance on an individual's movements, including from times when they were not even a suspect for law enforcement.[34] Without Clearview's technology, this type of surveillance would be cost prohibitive for law enforcement using traditional investigative techniques.[35] The public does not expect police to secretly monitor and catalogue their every movement, or be able to retrace their whereabouts easily and instantly.[36] And Clearview's database turns people's cameras and smartphones into advanced surveillance tools by allowing for the identification of individuals captured in others' photos without consent.[37] This technology circumvents "natural human privacy barriers" and reveals intimate offline information in which there is a reasonable expectation of privacy.[38]

By recognizing both user-driven indications of intent and traditional expectations against mass surveillance of physical movements, courts can reaffirm that privacy interests in biometric data are not only reasonable but squarely within the protections Proposition 11 was meant to secure.

A serious invasion of the protected interest

Determining how Clearview's use of our biometric information constitutes a serious invasion of privacy presents another challenge. As *Hill* observed, "[c]omplete privacy does not exist in this world except in a desert[.]"[39] After all, faces are visible in public, and being seen on the street is not itself an invasion. But online permanence alters the equation. Clearview's technology exploits that permanence, converting transient public observations into enduring, inescapable biometric records. Once entered into its database, an individual "permanently loses anonymity and privacy."[40] Unlike passwords or financial data, biometric faceprints cannot be reset, changed, or concealed. Clearview's technology therefore creates a permanent loss of control over an individual's biometric information. The result is profound: a person's identity and associations can be monitored indefinitely, their movements traced, and their records misused for stalking or identity theft. This loss of control over one's identity and associations strikes at the core concern of Proposition 11. In

interpreting the scope of the newly crafted privacy amendment, *Valley Bank* assumed "that the right of privacy extends . . . to the details of one's personal life."[41] Clearview's practices intrude precisely on those details, creating a serious invasion of biometric privacy interests.[42]

Public policy reinforces the same conclusion. Proposition 11 arose from the recognition that advancing technology would erode freedom unless there were legally enforceable limits.[43] This reality holds true today: companies like Clearview AI will not protect our biometric information absent legal compulsion. In 1972, the arguments in favor of the ballot initiative framed the ability to control the government and business records kept on us as fundamental to controlling our personal lives.[44] The misuse of our biometric information poses a direct threat to that control. Without judicial enforcement, Californians risk losing it altogether. Californians need control back, and there must be a modern path for enforcing the constitutional right to privacy over this type of information. By finding that Clearview AI's practices violate the constitutional right to privacy, California courts could empower individuals to control dataflow and revive crucial privacy rights in the state.

The countervailing interest

If the court agrees that plaintiffs have satisfied the threshold inquiry for a cognizable privacy claim, it will turn to whether Clearview has alleged a sufficient justification for its privacy invasion. The standard for evaluating Clearview's justification, set out in *Hill,* depends on "the specific kind of privacy interest involved and the nature and seriousness of the invasion and any countervailing interests."[45] Two potential standards apply. If the privacy interest is deemed fundamental to personal autonomy, Clearview must show a compelling countervailing interest to justify its practices.[46] If the interest at stake is less central, the court applies only a general balancing test.[47]

Since *Hill,* the California Supreme Court has rarely invoked the compelling interest test.[48] The only recent case employing it involved consent requirements on pregnant

minors seeking abortions, which is deeply tied to bodily autonomy.[49] Yet the court has acknowledged that personal autonomy in the privacy context is not limited only to matters of bodily integrity but can extend to matters affecting self-determination.[50] Even under this expanded view, it is not clear whether *Renderos* implicates autonomy interests. Clearview's information gathering could implicate interests in freedom of expression and association similar to those at issue in *White*, which required a compelling interest. But *Hill* limited *White*'s reach to "obvious government action" directly burdening those freedoms, noting that the judicial assessment of countervailing interests "may differ in cases of private, as opposed to government, action."[51] Ultimately, because Clearview is a private actor that does not compel action or impose restrictions on plaintiffs' movements, the court is more likely to opt for the general balancing test here.

Clearview likely will argue that its practices further the public interest in reducing crime and enhancing safety by helping law enforcement identify and locate suspected criminals, victims, and persons of interest. It raised a similar claim in its anti-SLAPP motion, but the appellate court rejected it, noting that this public interest is advanced by Clearview's government customers, not Clearview itself.[52] As a for-profit corporation, Clearview's motivations for gathering and storing biometric information are commercial. On the other side of the scale is the seriousness of the privacy invasion: the potential permanent loss of anonymity, exposure to misidentification, and the covert collection and retention of immutable biometric data without consent. On balance, plaintiffs should prevail.[53] Rejecting Clearview's justifications would reaffirm that commercial data practices cannot override core privacy interests.

Conclusion

The arguments in favor of Proposition 11 warned of snooping, secret data gathering, and the loss of control over our private information as serious threats to freedom. In the decades since then California courts have strayed from its constitutional purpose. *Renderos v. Clearview AI* presents an opportunity for California courts to reinvigorate the state constitutional right to privacy in the AI age. By recognizing

biometric surveillance as a serious invasion of privacy, the court can vindicate the fears expressed in 1972, restore to Californians the control they were originally promised, and reaffirm California's role as a national leader in privacy protection. Otherwise, Californians may be left behind without recourse against increasingly concerning invasions by the government and private entities. However the court rules, *Renderos* has set the stage for California to show the right to privacy is more than a paper promise.

—o0o—

Morgan Mitruka is a senior research fellow at the California Constitution Center.

1. *See* Nicole 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* (2024) 39 Berkeley Tech. L.J. 961, 966–67. ↑
2. Ballot Pamp., General Elec. (Nov. 7, 1972) at 27 [hereinafter "Ballot Pamp."]. ↑
3. *Id.* ↑
4. White v. Davis (1975) 13 Cal.3d 757, 760. ↑
5. Valley Bank v. Superior Court (1975) 15 Cal.3d 652, 654. ↑
6. Hill v. Nat'l Collegiate Athletic Ass'n (1994) 7 Cal.4th 1, 9. ↑
7. *Id.* at 35–37. ↑
8. *See, e.g.,* David A. Carrillo, Stephen M. Duvernay, Rodolfo Rivera Aquino & Brandon V. Stracener, *California Constitutional Law: Privacy* (2022) 59 San Diego L. Rev. 119, 134–35. ↑
9. *See* Rodolfo Rivera Aquino, *California's constitutional privacy guarantee needs a reset* (April 9, 2021) SCOCAblog.com. ↑
10. *Id.* ↑

11. *See, e.g.*, Mastel v. MINICLIP SA (E.D.Cal. 2021) 549 F.Supp.3d 1129, 1142; Cahen v. Toyota Motor Corp. (N.D.Cal. 2015) 147 F.Supp.3d 955, 958; In re iPhone Application Litig. (N.D.Cal. 2012) 844 F.Supp.2d 1040, 1049; Low v. LinkedIn Corp. (N.D.Cal. 2012) 900 F.Supp.2d 1010, 1025. ↑

12. *See* Robert Hart, *Clearview AI—Controversial Facial Recognition Firm—Fined $33 Million for 'Illegal Database'* (Sept. 3, 2024) Forbes; Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It* (Jan. 18, 2020) N.Y. Times (hereinafter "*The Secretive Company*"); Joel McConvey, *Canadian court upholds Clearview biometric data ban* (Jan. 10, 2025) BiometricUpdate.com. ↑

13. First Am. Compl., Renderos et al. v. Clearview AI, Inc. (Alameda Cty Super. Ct. Dec. 16, 2022) No. RG21096898 (hereinafter "First Am. Compl."). ↑

14. *Id.* at ¶ 4. ↑

15. *Id.* at ¶¶ 5, 41. ↑

16. *Id.* at ¶ 70. ↑

17. Renderos et al. v. Clearview AI, Inc. (Cal. Ct. App. May 22, 2025) No. A167179. ↑

18. *See* Branzburg v. Hayes (1972) 408 U.S. 665, 691 ("It would be frivolous to assert . . . that the First Amendment, in the interest of securing news or otherwise, confers a license on either the reporter or his news sources to violate valid criminal laws."). ↑

19. *White*, 13 Cal.3d at 770, 774 ("Because the identity of such police officers is unknown, no professor or student can be confident that whatever opinion he may express in class will not find its way into a police file."). ↑

20. Press release, *FTC Warns About Misuses of Biometric Information and Harm to Consumers* (May 18, 2023) Federal Trade Commission. ↑

21. *See* Katja Kukielski, *The First Amendment and Facial Recognition*

Technology (2022) 55 Loy. L.A. L. Rev. 231, 243–45; *see also White*, 13 Cal.3d at 767. ↑

22. *See* Jannice Cebreros, *Facial Recognition Technology and Wrongful Arrests in the Digital Policing Era* (2025) 100 Wash. L. Rev. Online 33, 39. ↑

23. Press release, *Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Reasonable Safeguards* (Dec. 19, 2023) Federal Trade Commission. ↑

24. *See* Kukielski at 244. ↑

25. *See White*, 13 Cal.3d at 761. ↑

26. *Hill*, 7 Cal.4th at 37. ↑

27. *See* Colleen McClain, Michelle Faverio, Monica Anderson & Eugenie Park, *How Americans View Data Privacy* (Oct. 18, 2023) Pew Research Center. ↑

28. *See* Bobby Allyn, *With no federal facial recognition law, states rush to fill void* (Aug. 28, 2025) NPR; Afshan Bhatia, Anokhy Desai, Kewa Jiang & Hina Moheyuddin, *AI and Privacy: A Guide to California's Recently Passed Legislation* (Sept. 18, 2025) California Lawyers Association. ↑

29. *Google, YouTube, Venmo and LinkedIn send cease-and-desist letters to facial recognition app that helps law enforcement* (Feb. 5, 2020) CBS News. ↑

30. *See, e.g.*, In re Facebook, Inc. Internet Tracking Litigation (9th Cir. 2020) 956 F.3d 589, 602–03. ↑

31. *The Secretive Company.* ↑

32. *See* Carpenter v. U.S. (2018) 585 U.S. 296, 310 ("[I]ndividuals have a reasonable expectation of privacy in the whole of their physical movements."). ↑

33. Kevin Johnson, *The Use of Clearview AI to Support Warrants Violates the Fourth Amendment*, 34 Fordham Intell. Prop. Media & Ent. L.J. 991, 1027. ↑

34. *Id.* at 1025 ("It's as if the police were watching the individual the entire time, even though at the time the photo was harvested the individual was not suspected of any wrongdoing."). ↑

35. *Carpenter*, 585 U.S. at 312. ↑

36. *Id.* at 311–12. ↑

37. *See* Johnson at 1026. ↑

38. *Id.* at 1016. ↑

39. *Hill*, 7 Cal.4th at 37 (internal citation omitted). ↑

40. First Am. Compl. at ¶ 89. ↑

41. *Valley Bank*, 15 Cal.3d at 656. ↑

42. *See, e.g.*, Patel v. Facebook, Inc. (9th Cir. 2019) 932 F.3d 1264, 1273 (finding Facebook's similar biometric data practices invade an individual's private affairs and concrete interests). ↑

43. *See also Valley Bank*, 15 Cal.3d at 657. ↑

44. *See* Ballot Pamp. at 27. ↑

45. *Hill*, 7 Cal.4th at 34. ↑

46. *See* Williams v. Superior Court (2017) 3 Cal.5th 531, 556. ↑

47. *See id.* ↑

48. Lewis v. Superior Court (2017) 3 Cal.5th 561, 573. ↑

49. *See* American Academy of Pediatrics v. Lungren (1997) 16 Cal.4th 307, 337. ↑

50. *See* Matthews v. Becerra (2019) 8 Cal.5th 756, 782. ↑

51. *Hill*, 7 Cal.4th at 34, 38. ↑

52. *See Renderos*, No. A167179. ↑

53. *See* Hernandez v. Hillsides, Inc. (2009) 47 Cal.4th 272, 300. ↑