November 28, 2023

VIA EMAIL AND FEDERAL EXPRESS

The Honorable Rob Bonta
Attorney General
State of California
Department of Justice
1300 I Street
Sacramento, CA 95814
Rob.Bonta@doj.ca.gov
(916) 445-9555

Ashkan Soltani
Executive Director
California Privacy Protection Agency
2101 Arena Boulevard
Sacramento, CA 95834
Ashkan.Soltani@cppa.ca.gov
(916) 572-2900

Re: Take Action Against Clearview AI's Flagrant Violations of California Law

Dear Attorney General Bonta and Executive Director Soltani,

Clearview AI's facial recognition software represents a clear and present danger to our societal norms and our privacy. It is time for California's top cop and the nation's premier privacy protection agency to act. A moratorium on the use of facial recognition technology in California ended at the beginning of the year, and state lawmakers failed to pass new protections in the recently-ended Legislative session. However, existing laws give you the power to protect Californians from these privacy threats, including that:

- **Clearview AI is unable to comply with the "right to opt out" provisions of the California Consumer Privacy Act.** Clearview AI technology functions by automatically scraping images off the web without regard for whose images are being scraped or whether the scraped images are of people who have previously prohibited Clearview AI from using or disclosing their biometric information. Therefore, Clearview AI appears to be violating "opt out" requirements of California law, since people who direct Clearview AI to remove their data cannot prevent their image from being re-appropriated by Clearview AI.

- **Clearview AI flouts laws designed to protect the personal data of children.** Certain provisions of the California Consumer Privacy Act and its implementing regulations require special handling of the personal information of individuals under the age of sixteen and prohibit businesses from selling or sharing the personal data of children without affirmative consent. If Clearview AI is incapable of obtaining consent to use the personal data of minors (as it has claimed), the solution is not to continue to allow Clearview AI to flout the law, but to prevent Clearview AI from continuing to violate the rights of California's children by shutting down Clearview AI's illegal data collection operations altogether.

- **Clearview AI promotes its technology to law enforcement even though the technology infringes upon Constitutionally-protected rights.** "Evidence suggests [facial recognition technology] may be least accurate on those it is most likely to be used on—African Americans."[1] The "real-world consequences" of such errors include "the investigation and arrest of an unknown number of innocent people and the deprivation of due process of many, many more."[2]

Consumer Watchdog provides the attached report on Clearview AI's use of facial recognition technology and an analysis of the accompanying legal violations. We urge you to use all the powers available to your offices to enjoin the use of Clearview AI's facial recognition technology by any public agency or department, and to take all punitive action deemed appropriate in light of Clearview AI's repeated and flagrant violations of law. Doing so will demonstrate your commitment to protecting the rights of California's citizens and preventing the unwarranted "encroachment on personal freedom and security caused by increased surveillance and data collection activity" that voters so many years ago sought to prohibit with their 1972 amendment to the California Constitution guaranteeing the inalienable right to "pursue and obtain privacy."[3]

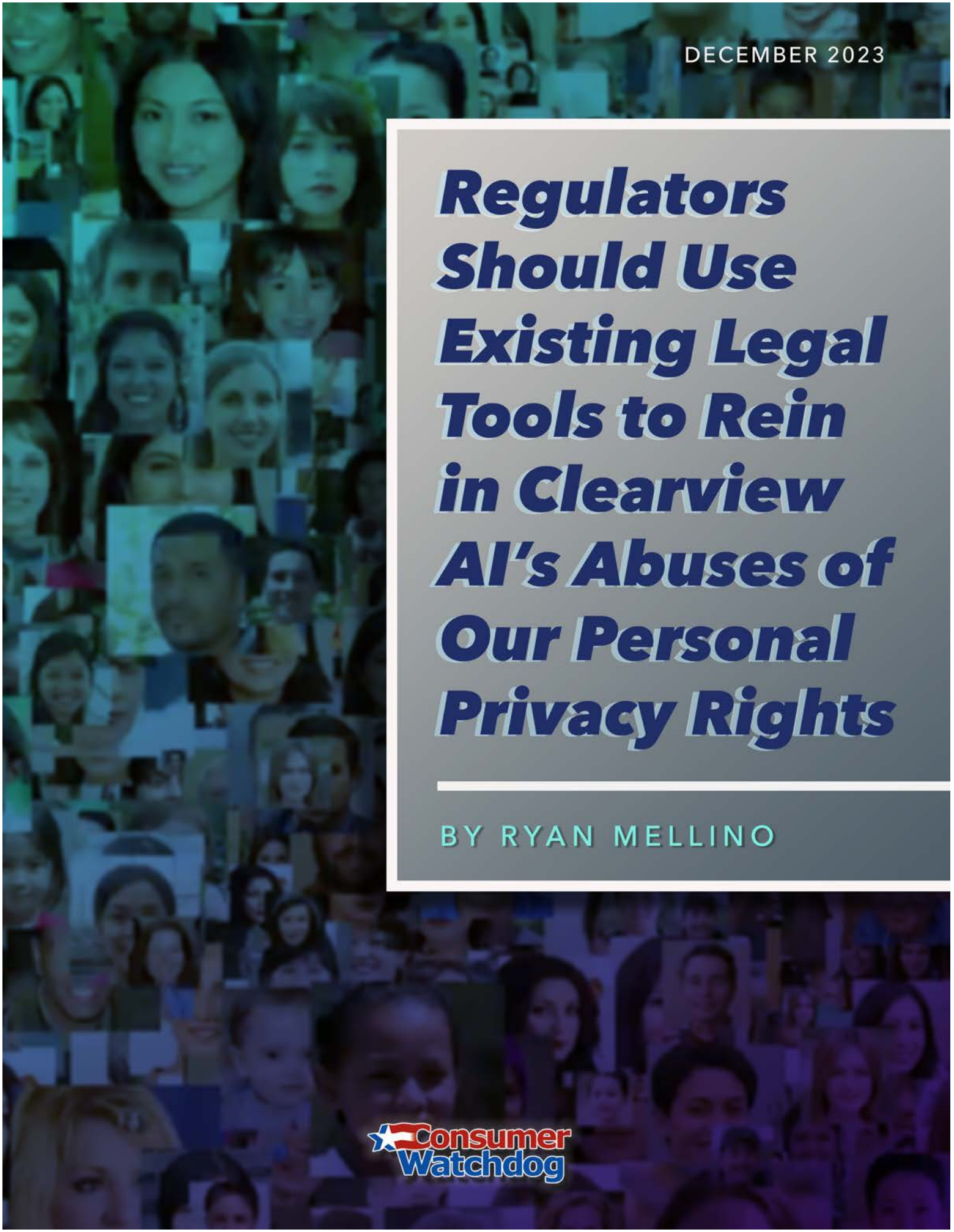
We may be reached at 310-392-0522 ext. 115 and via email.

Sincerely,

Ryan Mellino
Staff Attorney
Ryan@consumerwatchdog.org

Benjamin Powell
Staff Attorney
Ben@consumerwatchdog.org

[1] *Police Face Recognition Technology*, Georgetown University Law Center, Center on Privacy and Technology, accessed Nov. 17, 2023, https://drive.google.com/file/d/1trfTqLQXW4MOyQoxaMSmrF02kz-DC6MU/view.
[2] Newsletter, *A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations*, Georgetown University Law Center, Center on Privacy and Technology, accessed Nov. 17, 2023, https://www.law.georgetown.edu/privacy-technology-center/publications/a-forensic-without-the-science-face-recognition-in-u-s-criminal-investigations/.
[3] *White v. Davis* (1975) 13 Cal.3d 757, 774.



DECEMBER 2023

Regulators Should Use Existing Legal Tools to Rein in Clearview AI's Abuses of Our Personal Privacy Rights

BY RYAN MELLINO

Consumer Watchdog

Table of Contents

I. Introduction

In its very first provision, the California Constitution guarantees citizens the inalienable right to "pursue and obtain privacy."[1] The result of a voter-driven amendment in 1972, our state Supreme Court recognized that "the moving force behind the new constitutional provision was a more focussed privacy concern, relating to the accelerating encroachment on personal freedom and security caused by increased surveillance and data collection activity in contemporary society," and that the "provision's primary purpose is to afford individuals some measure of protection against this most modern threat to personal privacy."[2]

In contravention of these principles, Clearview AI has developed facial recognition technology capable of covertly and remotely identifying California citizens *en masse*. Rather than seek out individuals that would choose to allow Clearview AI to add their photographs to its database and use them for its own commercial purposes, Clearview AI instead covertly "scrapes" photographs (including personal profile images) from sources online, often from social media websites in contravention of user agreements (as discussed *infra*).[3] Clearview AI then adds these photos to its database that powers its entire commercial operation. Armed with billions of images, Clearview AI applies its facial recognition algorithm to create a vast dossier of "facial maps" from the scraped images.[4] The algorithm converts facial geometry—such as the space between one's eyes—into mathematical formulas and stores that information in a database organized by photos with similar geometry.[5] When a Clearview AI customer uploads a photo, "the system analyzes a face for

"From its beginnings, Clearview AI has operated with callous disregard for the privacy rights of individual citizens."

[1] Cal. Const. Art. I § 1.

[2] *White v. Davis* (1975) 13 Cal.3d 757, 774.

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

[4] *Ibid.*

[5] *Ibid.*

Hoan Ton-That, founder of Clearview AI, whose app matches faces to images it collects from across the internet. (Amr Alfiky, The New York Times)

particular measurements and ratios," "the image is compared to a database of known or existing faces," and photos are returned of the person along with links to where the photo came from.[6] Clearview AI advertised itself to potential clients as "like Google search for faces."[7] Federal lawmakers have noted that amongst facial recognition tools, "Clearview AI's product is particularly dangerous."[8]

From its beginnings, Clearview AI has operated with callous disregard for the privacy rights of individual citizens. As stated by NPR, "the company didn't want you to know it existed," and "did its best to remain secretive until it was exposed" by *New York*

---

[6] Beryl Lipton, *Records on Clearview AI reveal new info on police use*, Muckrock, Jan. 18, 2020, https://www.muckrock.com/news/archives/2020/jan/18/clearview-ai-facial-recogniton-records/.

[7] Chula Vista Police Department Response to 12/20/20 Muckrock CPRA Request, CL PRA 5, p. 1, accessed Nov. 11, 2023, https://cdn.muckrock.com/foia_files/2021/02/11/CL_PRA_5.pdf.

[8] U.S. Senators Edward J. Markey and Jeffrey A. Merkley & U.S. Representatives Pramila Jayapal and Ayanna Pressley, Letter to DHS Secretary Alejandro Mayorkas Regarding Clearview AI, p. 1, Feb. 9, 2022, https://www.markey.senate.gov/imo/media/doc/letters_-_federal_gov_use_of_clearview_ai.pdf.

Times reporter Kashmir Hill in January 2020.[9] Another commentator described Clearview AI as a "secretive startup that, until January 2020, was virtually unknown to the public, despite selling [a] state-of-art facial recognition system to cops and corporations."[10] Throughout that time, Clearview AI aggressively marketed itself to law enforcement agencies. A September 10, 2019 email "on behalf of Team Clearview" to an agent with the Chula Vista Police Department exhorted the agent to do three things: "[s]earch a lot," "[r]efer your colleagues," and "[g]et Clearview for the long haul," and challenged the agent to "[s]ee if you can reach 100 searches."[11] A subsequent October 28, 2019 email from Jack Mulcaire with Clearview AI[12] to the same agent requested a phone call regarding "how to make your department a permanent user of Clearview."[13]

Mr. Ton-That showing the results of a search for a photo of himself. (Amr Alfiky, The New York Times)

---

[9] Terry Gross, *Exposing the secretive company at the forefront of facial recognition technology*, NPR, Sept. 28, 2023, https://www.npr.org/2023/09/28/1202310781/exposing-the-secretive-company-at-the-forefront-of-facial-recognition-technology.

[10] Nilay Patel, *Clearview AI and the end of privacy, with author Kashmir Hill*, The Verge, Oct. 17, 2023, https://www.theverge.com/23919134/kashmir-hill-your-face-belongs-to-us-clearview-ai-facial-recognition-privacy-decoder.

[11] Chula Vista Police Department Response to 12/20/20 Muckrock CPRA Request, CL PRA 3, p. 5, accessed Oct. 24, 2023, https://cdn.muckrock.com/foia_files/2021/02/11/CL_PRA_3.pdf.

[12] Jack Mulcaire appears to be a name used by Clearview AI's current general counsel, Thomas Jackson Mulcaire, Cal. SBN # 330867. (Compare Christina Tabacco, *Clearview AI Asks Court to Take Second Look at Dismissal Order in Biometric Information Privacy MDL*, Law Street Media, Mar. 16, 2022, https://lawstreetmedia.com/news/tech/clearview-ai-asks-court-to-take-second-look-at-dismissal-order-in-biometric-information-privacy-mdl/ [referring to Clearview AI's general counsel as Thomas Mulcaire]; with Emma Woollacott, *U.K. Privacy Watchdog Can't Sanction Clearview AI, Court Rules*, Forbes, Oct. 19, 2023, https://www.forbes.com/sites/emmawoollacott/2023/10/19/uk-privacy-watchdog-cant-sanction-clearview-ai-court-rules/?sh=504b5b987e39 [referring to Clearview AI's general counsel as Jack Mulcaire].) Mulcaire was apparently not "licensed as an attorney [until] March, 2020 . . . even though he claimed to have been Clearview General Counsel since September 2019 on three occasions." (Chris Burt, *Clearview accused of attempting to move biometric data beyond reach of US law*, BiometricUpdate.com, May 20, 2021, https://www.biometricupdate.com/202105/clearview-accused-of-attempting-to-move-biometric-data-beyond-reach-of-us-law.)

[13] See fn. 7, p. 139.

II. Need for Regulators to Take Strong Action Now

Action is necessary given the recent lapse of California's three-year moratorium on the use of facial recognition technology by law enforcement. Enacted by A.B. 1215 in 2019, the moratorium stated: "Facial recognition and other biometric surveillance technology pose unique and significant threats to the civil rights and civil liberties of residents and visitors."[14] What's more, the bill recognized that the "use of facial recognition and other biometric surveillance is the functional equivalent of requiring every person to show a personal photo identification card at all times in violation of recognized constitutional rights."[15] The bill further noted: "The use of facial recognition and other biometric surveillance would disproportionately impact the civil rights and civil liberties of persons who live in highly policed communities."[16] This technology has a chilling effect, especially on people of color, who may be "deterr[ed] from participating in marches or rallies, or speaking out against injustice, for fear of being permanently included in law enforcement databases."[17] "Studies show that when individuals believe the government is surveilling them, they are likely to avoid engaging in activities protected by the First Amendment."[18]

Thus, California has already recognized the illegality inherent in Clearview AI's actions: the "use of facial recognition and other biometric surveillance is the functional equivalent of [a] violation of recognized constitutional rights."[19] The state further recognized the disproportionate impact biometric surveillance technology usage would have on disadvantaged communities, given the fact that "[f]acial recognition and other biometric surveillance technology has been repeatedly demonstrated to misidentify women, young people, and people of color and to create an elevated risk of harmful 'false positive' identifications."[20] Yet, after the moratorium ended in 2023, the legislature was

---

[14] Assem. Bill No. 1215 (2019–2020 Reg. Sess.) § 1, subd. (b), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1215.

[15] *Id.*, § 1, subd. (c).

[16] *Id.*, § 1, subd. (f).

[17] See fn. 8, pp. 1–2 (also noting that "past law enforcement use of [facial recognition] technology reportedly targeted Black Lives Matter activists").

[18] *Id.* at p. 1.

[19] See fn. 14, § 1, subd. (c).

[20] *Id.*, § 1, subd. (d).

unable to come together to pass any legislation either regulating or prohibiting the use of facial recognition technology in California, with two bills on the issue failing to reach a floor vote in 2023 (A.B. 642 and A.B. 1034).[21]

Additionally, although many tech companies, including Google, Facebook, Twitter, YouTube, Venmo, and LinkedIn, sent cease-and-desist letters to Clearview AI in 2020 demanding that it stop scraping data in violation of the applicable terms of service,[22] Clearview AI does not appear to have complied with any of those demands, nor do the tech companies appear to have taken any direct action against Clearview AI to enforce their demands. Thus, despite apparent agreement in both the public and private sectors that Clearview AI has violated the law, neither sector has taken any real enforcement action since the moratorium was initially put in place.

It is crucial that the Attorney General's office and the California Privacy Protection Agency use their power to protect California citizens from these grievous violations of their privacy rights. Citizens' rights to sue under the California Consumer Privacy Act ("CCPA") are limited to cases involving data breaches.[23] The Attorney General is empowered to fully enforce the provisions of the CCPA,[24] as well as to challenge Clearview AI's other violations of law. In these circumstances, it is incumbent upon the Attorney General's Office as the "state's top lawyer and law enforcement official" to fulfill your "responsibilit[y to] safeguard[] Californians from harm,"[25] and to continue to show you are "committed to the robust enforcement of the CCPA."[26]

---

[21] Assem. Bill No. 642 (2023–24 Reg. Sess.), https://legiscan.com/CA/text/AB642/id/2796168; Assem. Bill No. 1034 (2023–24 Reg. Sess.), https://legiscan.com/CA/text/AB1034/id/2796150.

[22] *Google, YouTube, Venmo and LinkedIn send cease-and-desist letters to facial recognition app that helps law enforcement*, CBS News, Feb. 5, 2020, https://www.cbsnews.com/news/clearview-ai-google-youtube-send-cease-and-desist-letter-to-facial-recognition-app/; Alfred Ng & Steven Musil, *Clearview AI hit with cease-and-desist from Google, Facebook over facial recognition collection*, CNET, Feb. 5, 2020, https://www.cnet.com/news/privacy/clearview-ai-hit-with-cease-and-desist-from-google-over-facial-recognition-collection/.

[23] Civ. Code § 1798.150.

[24] See Civ. Code § 1798.199.90.

[25] About the Office of the Attorney General, California Department of Justice, https://oag.ca.gov/office.

[26] *Attorney General Bonta Seeks Information from California Employers on Compliance with California Consumer Privacy Act*, California Department of Justice, July 14, 2023, https://oag.ca.gov/news/press-releases/attorney-general-bonta-seeks-information-california-employers-compliance.

Similarly, the California Privacy Protection Agency has the authority to bring certain enforcement actions to collect fines for violations of the CCPA,[27] and is also permitted to open investigations or audits of any business to determine if it is in compliance with the CCPA.[28] The California Privacy Protection Agency must fulfill its "mission . . . to protect consumer privacy . . . and vigorously enforce the California Consumer Privacy Act."[29] Indeed, as the "first government body in the United States with the sole job of regulating how . . . companies collect and use data from millions of people," there is no other agency in the country with comparable power to enforce our privacy rights.[30] In 2020, the International Association of Privacy Professionals opined that "the [California Privacy Protection Agency] is set to become a key privacy regulator not only in California, but across the U.S. and the globe."[31] Given the inability of data protection authorities in other countries to effectively enforce their laws against Clearview AI (see *infra*), the California Privacy Protection Agency can take its place as a "key privacy regulator across the globe" by confronting Clearview AI's flagrant violations of personal privacy.

[27] Civ. Code § 1798.155.

[28] 11 Cal. Code Regs. §§ 7301, 7304.

[29] Frequently Asked Questions, California Privacy Protection Agency, accessed Nov. 17, 2023, https://cppa.ca.gov/faq.html.

[30] David McCabe, *How California Is Building the Nation's First Privacy Police*, The New York Times, Mar. 15, 2022, https://www.nytimes.com/2022/03/15/technology/california-privacy-agency-ccpa-gdpr.html.

[31] Lydia de la Torre & Glenn Brown, International Association of Privacy Professionals, *What is the California Privacy Protection Agency?*, The Privacy Advisor, Nov. 23, 2020, https://iapp.org/news/a/what-is-the-california-privacy-protection-agency/.

III. Use of Clearview AI by Law Enforcement

While Clearview AI is barred from selling its product to private businesses under a nationwide injunction entered pursuant to a settlement agreement in the case *ACLU v. Clearview AI, Inc.* (Ill. Cir. Ct., May 11, 2022) No. 20 CH 4353, no statewide restrictions currently apply to Clearview AI's ability to contract with or sell its technology to government and law enforcement agencies in California.[32] Nor is there any law specifically directed at regulating the use of such technology by government agencies or law enforcement. Similarly, a recent Executive Order issued on Artificial Intelligence, while stating important principles of privacy regulation, is inapplicable at the state or local agency level.[33] Moreover, Clearview AI continues to collect data and images in violation of California law. In this absence of legislative action, it is incumbent upon you to enforce the laws California already has that bar Clearview AI's unlawful actions.

While it is unclear just how widespread the usage of Clearview AI by government agencies is today, in March 2023, CEO Hoan Ton-That told the BBC that Clearview AI had run around one million searches for law enforcement agencies throughout the United States.[34] One law review article notes that "[a]s of June 2021, more than half of all adults in the United States are in facial recognition databases used for criminal investigations, and Clearview AI advertises they have enough photos in their database to make 'almost everyone in the world…identifiable.'"[35] This lack of transparency concerning, and regulation of, this technology cannot be tolerated.

Thus, agencies and law enforcement departments cannot be left to their own devices to determine whether and how to use this technology. For example, the Los Angeles Police Department put policies into place governing the use of facial recognition

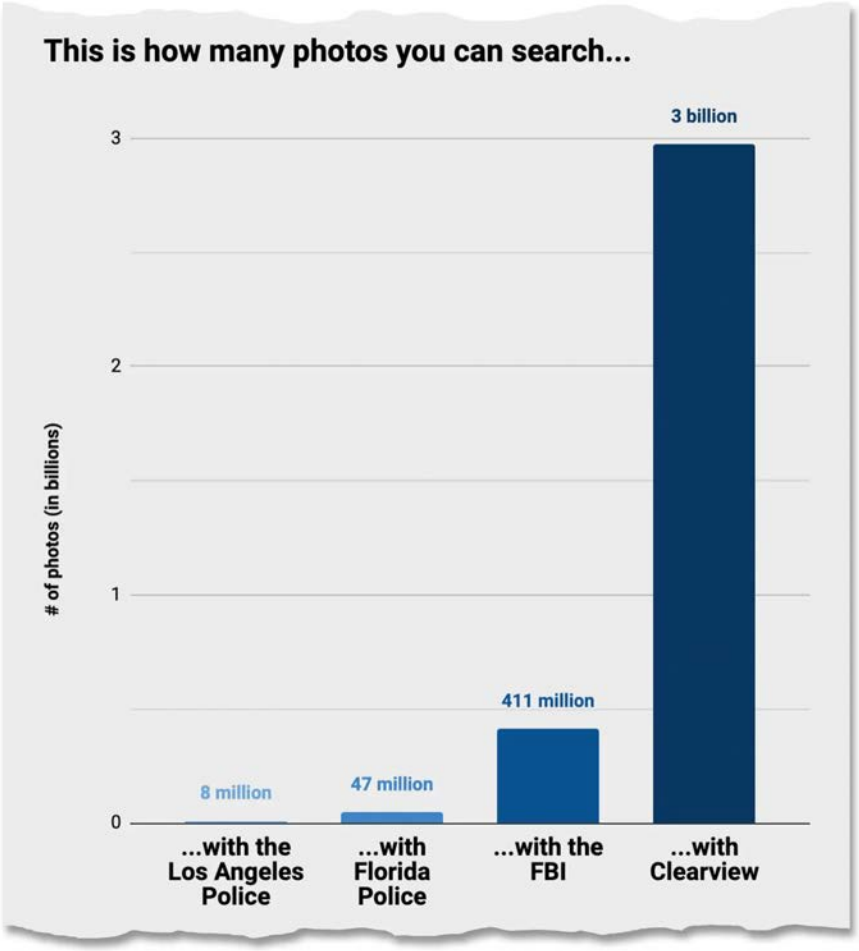
---

[32] Clearview AI, *What Law Enforcement Should Know Before Using Facial Recognition Technology in California*, Nov. 30, 2022, https://www.clearview.ai/post/what-law-enforcement-should-know-before-using-facial-recognition-technology-in-california.

[33] Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, Oct. 30, 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

[34] James Clayton & Ben Derico, *Clearview AI used nearly 1m times by US police, it tells the BBC*, BBC News, Mar. 27, 2023, https://www.bbc.com/news/technology-65057011.

[35] Emilia Ball, *Facial Recognition in the Eyes of the Law*, 2023 B.C. Intell. Prop. & Tech. F. 1, October 30, 2023, at 2.



A chart from marketing materials that Clearview AI provided to law enforcement.

technology in January 2021.[36] Yet a December 2022 report by the LAPD Inspector General found that the "department lacks a way to track [facial recognition technology's] outcomes or effectiveness."[37] The report noted there was "'no way to verify or analyze the search results,'" or to determine how many times the technology may have misidentified an individual.[38] The Department further lacked the ability to determine whether officers were following certain laws and policies concerning the use of such technology.[39]

---

[36] Libor Jany, *LAPD doesn't fully track its use of facial recognition, report finds*, Los Angeles Times, Dec. 14, 2022, https://www.latimes.com/california/story/2022-12-14/lapd-doesnt-fully-track-its-use-of-facial-recognition-report-finds.

[37] *Ibid.*

[38] *Ibid.*

[39] *Ibid.*

IV. False Positive Identifications Are Unavoidable

Although Clearview AI "often points to research that shows it has a near 100% accuracy rate . . . [i]n reality, the accuracy of Clearview depends on the quality of the image that is fed into it - something Mr Ton-That accepts."[40] And despite Clearview AI's touting of a near 100% accuracy rate, Ton-That in fact "does not want to testify in court to its accuracy," arguing that "'investigators [are] using other methods to also verify it.'"[41] Notwithstanding Ton-That's claims, unsurprisingly, "[e]vidence suggests [facial recognition technology] may be least accurate on those it is most likely to be used on—African Americans."[42] The moratorium previously enacted by California's legislature similarly recognized that "[f]acial recognition and other biometric surveillance technology has been repeatedly demonstrated to misidentify women, young people, and people of color and to create an elevated risk of harmful 'false positive' identifications."[43]

Indeed, a recent report published by the Georgetown University Law Center's Center on Privacy and Technology highlighted problems with the use of facial recognition technology by law enforcement, including that "[a]s a biometric, forensic investigative tool, face recognition may be particularly prone to errors arising from subjective human judgment, cognitive bias, low-quality or manipulated evidence, and under-performing technology."[44] The report noted the "real-world consequences" of such errors, including "the investigation and arrest of an unknown number of innocent people and the deprivation of due process of many, many more."[45] Despite widespread concerns over the propensity of facial recognition technology to misidentify minority individuals in particular, the report states that "face recognition has been used as probable cause to make arrests," and that "[i]n a number of cases across multiple jurisdictions, people have

---

[40] See fn. 34.

[41] *Ibid.*

[42] *Police Face Recognition Technology*, Georgetown University Law Center, Center on Privacy and Technology, accessed Nov. 17, 2023, https://drive.google.com/file/d/1trfTqLQXW4MOyQoxaMSmrF02kz-DC6MU/view.

[43] See fn. 14.

[44] Newsletter, *A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations*, Georgetown University Law Center, Center on Privacy and Technology, accessed Nov. 17, 2023, https://www.law.georgetown.edu/privacy-technology-center/publications/a-forensic-without-the-science-face-recognition-in-u-s-criminal-investigations/.

[45] *Ibid.*

found themselves jailed and facing criminal charges based on a face recognition search alone; no other evidence was sought to confirm the suspect's identity."[46]

As a result, the report came to a forceful, inexorable conclusion: "face recognition doesn't work well enough to reliably serve the purposes for which law enforcement agencies themselves want to use it."[47] The report concludes with a call "to question any and all assumptions that the current use of face recognition is adequately controlled and reliable," and "warns that we have a narrow and closing window of time in which to [not] repeat the mistakes of previous forensic disciplines and avoid judicial certification of fundamentally flawed or unreliable methods."[48]

Clearview AI's marketing materials, obtained through a public-records request in Atlanta.

---

[46] Clare Garvie, *A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations*, Georgetown University Law Center, Center on Privacy and Technology (Dec. 6, 2022), p. 47, https://mcusercontent.com/672aa4fbde73b1a49df5cf61f/files/2c2dd6de-d325-335d-5d4e-84066159df71/Forensic_Without_the_Science_Face_Recognition_in_U.S._Criminal_Investigations.pdf.

[47] See fn. 44.

[48] *Ibid.*; see generally Samantha L. Shamhart, *The Mosaic Theory: How the Intersection of Mass Surveillance and Facial Recognition Is Provoking an Orwellian Future* (2023) 51 Cap. U. L. Rev. 504, 541 (detailing concerns over use of Clearview AI by law enforcement and concluding that "severe limitations should be placed on law enforcement's use of advanced facial recognition technology, such as Clearview AI").

V. Clearview AI Is Violating California Law

As one judge aptly noted, Clearview AI "forged ahead and blindly created billions of faceprints without regard to the legality of that process in all states."[49] That is certainly true as to California, where Clearview AI's actions have likely violated California's constitutional, statutory, and common law, such as the:

- Right to privacy guaranteed by the California Constitution, Article I, Section I;[50]
- California Consumer Privacy Act, Civil Code section 1798.100 et seq. as discussed in detailed in Section VI, infra;
- Common Law Intrusion Upon Seclusion/Tort of Intrusion;[51]
- Common Law Appropriation of Likeness/Right to Publicity;[52]
- Statutory Commercial Misappropriation of Likeness/Right of Publicity, California Civil Code section 3344;[53]
- Common Law Bad Faith Breach of Terms of Service;[54] and the

---

[49] *ACLU v. Clearview AI, Inc.* (Ill. Cir. Ct., Aug. 27, 2021) No. 20 CH 4353, Decision Denying Clearview AI's Motion to Dismiss, p. 12.

[50] See *In re Clearview AI, Inc., Consumer Priv. Litig.*, 585 F. Supp. 3d 1111, 1130 (N.D. Ill. 2022) (court found plaintiffs plausibly stated claim for violation of right to privacy under California Constitution); *Renderos v. Clearview AI, Inc.*, Cal. Super. Ct. No. RG21096898, Decision on Anti-SLAPP Motion, Nov. 18, 2022, p. 7 (plaintiffs stated plausible claim for invasion of privacy under California Constitution); *Ji v. Naver Corporation* (N.D. Cal., Oct. 3, 2023) No. 21-CV-05143-HSG, 2023 WL 6466211, at *9 (same).

[51] See *Ji*, *supra*, 2023 WL 6466211, at *9 (plaintiffs stated claim for intrusion upon seclusion based on "Defendants' alleged collection of content," including facial biometric information).

[52] See *In re Clearview AI*, *supra*, 585 F. Supp. 3d at p. 1129 (court found plaintiffs plausibly stated claim for right of publicity under California common law); *Renderos*, *supra*, Decision on Anti-SLAPP Motion, pp. 5–7 (plaintiffs plausibly stated claim for common law misappropriation of likeness).

[53] See *In re Clearview AI*, *supra*, 585 F. Supp. 3d at p. 1129 (court found plaintiffs plausibly stated claim for right of publicity under section 3344).

[54] See Benjamin L.W. Sobel, *A New Common Law of Web Scraping* (2021) 25 Lewis & Clark L. Rev. 147, 183 (arguing, in the context of Clearview AI, that the "common law of California can support a . . . claim against entities that willfully violate a platform's terms of service, to the detriment of claimants who rely on those same terms in separate agreements with the platform").

• Unfair Competition Law, Civil Code section 17200 *et seq.*[55]

Among the most egregious legal issues are Clearview AI's brazen violations of societal privacy norms. The California Supreme Court has evaluated claims of a violation of the right of privacy under the California Constitution and the common law tort of intrusion together in a two-part test where the court "consider[ed] (1) the nature of any intrusion upon reasonable expectations of privacy, and (2) the offensiveness or seriousness of the intrusion, including any justification and other relevant interests."[56] It is beyond dispute that a person's biometric information, "by its very nature, is sensitive and confidential,"[57] and therefore is something over which individuals have a reasonable expectation of privacy.[58]

"There may be no greater violation of societal expectations of privacy in recent history than Clearview AI's collection of tens of billions of biometric face scans without consent."

As for the "offensiveness or seriousness of the intrusion," there may be no greater violation of societal expectations of privacy in recent history than Clearview AI's collection of tens of billions of biometric face scans without consent for use in a "technology [that] could eliminate public anonymity

---

[55] See *Renderos*, *supra*, Decision on Anti-SLAPP Motion, p. 8 (plaintiffs adequately stated claim for violation of UCL "unlawful prong" via claims of invasion of privacy and misappropriation of likeness); *Ji*, *supra*, 2023 WL 6466211 at *9 (finding plaintiffs adequately alleged an economic injury sufficient for UCL standing because the "collection and use of their data deprived them of the benefit of their bargain and diminished the value of their personal data"); *Brooks v. Thomson Reuters Corporation* (N.D. Cal. Aug. 16, 2021) No. 21-CV-01418-EMC, 2021 WL 3621837, at *8–9 (the "sale of Plaintiffs' most private and personal information states a claim under the unfair prong of the UCL").

[56] *Hernandez v. Hillsides, Inc.* (2009) 47 Cal.4th 272, 288.

[57] *In re Clearview AI, Inc.*, *supra*, 585 F.Supp.3d at p. 1130.

[58] See also *Patel v. Facebook, Inc.* (9th Cir. 2019) 932 F.3d 1264, 1273 ("conclud[ing] that the development of a face template using facial-recognition technology without consent . . . invades an individual's private affairs and concrete interests").

in the United States."[59] Indeed, the California Supreme Court previously recognized that the "right to control the dissemination of [one's] image and actions" is a "key feature of privacy"—a right over which Clearview AI has unashamedly run roughshod.[60] As many commentators have noted, even as compared to the scraping of other information online, there is "something in particular about faces and what Clearview AI did with faces that everyone reacts differently to," with Kashmir Hill opining:

> *I just think it's so personal. Who we are is in our face. And this idea that anyone can snap a photo of us and suddenly know not just who we are and where we live and who our friends are, but dig up all these photos of us on the internet going back years and years. I think there's just something inherently privacy-invasive about that that just is more resonant for people than cookies or tracking what websites you've been to. It's really controlling your identity.*[61]

It is important to note that even companies like Google and Facebook, which are not "'traditionally that conservative when it comes to private information,'" "'developed this ability internally and decided not to release it.'"[62] As stated by Kashmir Hill: "'What these start-ups [including Clearview AI] had done wasn't a technological breakthrough; it was an ethical one. Tech giants had developed the ability to recognize unknown people's faces years earlier, but had chosen to hold the technology back, deciding that the most extreme version—putting a name to a stranger's face—was too dangerous to make widely available.'"[63]

---

[59] See fn. 8, p. 1; see also Sobel, *A New Common Law*, *supra*, 25 Lewis & Clark L. Rev. at p. 147 (noting the "Clearview AI facial recognition scandal is a monumental breach of privacy"); Katja Kukielski, *The First Amendment and Facial Recognition Technology* (2022) 55 Loyola L.A. L.Rev. 231, 278 (noting that facial recognition technology "presents real risks that threaten our ability to navigate the world with some degree of control over who we expose ourselves to," and "serves as yet another powerful tool for Big Data to tighten its grip on consumers").

[60] *Hernandez*, *supra*, 47 Cal.4th at p. 291.

[61] See fn. 10.

[62] *Ibid.*

[63] Kashmir Hill, *The Technology Facebook and Google Didn't Dare Release*, The New York Times, Sept. 11, 2023, https://www.nytimes.com/2023/09/09/technology/google-facebook-facial-recognition.html.

Furthermore, the use of Clearview AI by law enforcement officials implicates an infringement on the right to freedom of speech and freedom of assembly guaranteed by Article I, Sections 2(a) and 3(a) of the California Constitution.[64]

Clearview AI often touts and legally relies on the fact that it has compiled a database of biometric information using only "publicly available information."[65] This is completely irrelevant in California.[66] In fact, California has, by statute, explicitly stated that "'[p]ublicly available' does not mean biometric information collected by a business about a consumer without the consumer's knowledge."[67] All of the biometric data Clearview AI has collected on California residents was collected without their knowledge, and thus the information was not "publicly available" as a matter of law.[68]

---

[64] See, e.g., *In re Clearview AI, Inc. Consumer Privacy Litig.* (N.D. Ill., Mar. 23, 2022) No. 21-CV-0135, 2022 WL 870637, at *3 (finding plaintiffs' allegation that "municipal defendants' use of Clearview's database has a chilling effect on their right to speech and association" was sufficient to show a "reasonable possibility" of stating a claim under the California Constitution); *Renderos v. Clearview AI, Inc.*, Cal. Super. Ct. No. RG21096898, Decision on Demurrer, June 14, 2022, p. 4 (finding plaintiffs "adequately allege[d] a Liberty of Speech claim directly against El Segundo based on its actions in providing biometric data to Clearview and in using Clearview's services might chill legitimate speech").

[65] See, e.g., Speech by Hoan Ton-That, The Modern Public Square: The Free Flow of Information in the Age of Artificial Intelligence, June 14, 2022, https://www.clearview.ai/post/the-modern-public-square-the-free-flow-of-information-in-the-age-of-artificial-intelligence; Jon Porter, *Facebook and LinkedIn are latest to demand Clearview stop scraping images for facial recognition tech*, The Verge, Feb. 6, 2020, https://www.theverge.com/2020/2/6/21126063/facebook-clearview-ai-image-scraping-facial-recognition-database-terms-of-service-twitter-youtube (noting that "Ton-That argues that his company has a right to use the data, since it's publicly available"); *ACLU v. Clearview AI, Inc.*, *supra*, Clearview AI's Memorandum in Support of Motion to Dismiss, Oct. 7, 2020, p. 16 (arguing that "Clearview's collection and use of publicly-available photographs are protected under the First Amendment").

[66] This argument appears similarly misplaced even outside of California—see, e.g., *U.S. Dept. of Defense v. Federal Labor Relations Authority* (1994) 510 U.S. 487, 500 ("An individual's interest in controlling the dissemination of information regarding personal matters does not dissolve simply because that information may be available to the public in some form").

[67] Civ. Code § 1798.140, subd. (v)(2).

[68] See also *Renderos*, *supra*, Decision on Anti-SLAPP Motion, p. 5 (noting that the "biometric analysis and maintenance of [Clearview AI's] database is not 'speech,'" and that if "the biometric analysis and maintenance of the database is unlawful, then it would not become lawful because it was either preceded by the lawful collection of information from public sources or was subsequently communicated (sold) to law enforcement").

VI. Spotlight on Clearview AI's Violations of California Consumer Privacy Act

Clearview AI is flouting laws designed to protect personal data, particularly as concerns the data of children. Certain provisions of the CCPA and its implementing regulations require special handling of the personal information of individuals under the age of sixteen and prohibit businesses from selling or sharing the personal data of children without affirmative consent.[69] Clearview AI does not comply with these laws because, as it claims in its privacy policy: "Clearview does not have actual knowledge of the age of the persons in the photos it collects from the Internet. As such, Clearview does not knowingly sell or share personal information about consumers under the age of 16."[70] There is simply no world in which any reasonable person could believe that Clearview AI does not actually know that it is using the personal data of individuals under the age of sixteen. At best, Clearview AI is "willfully disregarding" the ages of the millions of children it has scraped images of, which constitutes "actual knowledge" under California law.[71]

As evidence, Clearview AI's own website contains an article titled "How Facial Recognition is Identifying Human Trafficking Victims," wherein Kevin Metcalf, President and Founder of the National Child Protection Task Force, is quoted as stating: "'When Clearview came along, that allowed us to search and identify who they are, where they are […] **I can attest for hundreds of kids who were identified using facial**

[69] See, e.g., Civ. Code § 1798.120, subd. (c); 11 Cal. Code Regs. §§ 7070–72.

[70] Clearview AI, Inc. Privacy Policy, Clearview AI, accessed on Nov. 17, 2023, https://www.clearview.ai/privacy-policy.

[71] Civ. Code § 1798.120, subd. (c).

recognition technology.'"[72] Clearview AI's website also prominently touts its role in solving child exploitation cases, including this statement: "'Clearview AI is often the only tool available to law enforcement that is **able to identify an anonymous child's photo**.'"[73] On the same page, Chris Johnson, Regional Human Exploitation & Trafficking Unit Detective, is quoted as saying: "'We were able to take one of the photographs from one of these online escort websites, upload it into Clearview, and, within seconds, **Clearview was able to identify that individual. It was a 16-year-old female juvenile** . . . .'"[74] As a featured speaker at a Federalist Society event in 2021, Ton-That stated: "'when you arrest a pedophile sometimes there's about a thousand photos of kids on their hard drive that they [law enforcement] don't know who they are . . . **they're able to triple their rate of IDing the victims, they might find them in a school photo or a band practice or at soccer practice** . . . .'"[75] The former Attorney General of Vermont, Thomas Donovan, criticized Clearview AI, "'particularly [its] **practice of collecting and selling children's facial recognition data**.'"[76] A Reuters article noted that one of Clearview AI's plans in 2022 was to "add enhancement tools to clean up search photos and potentially AI to generate younger and older depictions so that **someday seniors could be matched to childhood photos**."[77] A *New York Times* article reported: "Investigators say Clearview's tools allow them to learn the names or locations of minors . . . ."[78] "And as stated by Kashmir Hill: "[Clearview] was a powerful tool not just for identifying perpetrators but

---

[72] Freethink Media, *How Facial Recognition is Identifying Human Trafficking Victims*, Clearview AI, June 15, 2022, https://www.clearview.ai/post/how-facial-recognition-is-identifying-human-trafficking-victims, emphasis added.

[73] *Child Exploitation*, Clearview AI, accessed on Nov. 17, 2023, https://www.clearview.ai/child-exploitation, emphasis added.

[74] *Ibid.*, emphasis added.

[75] *Panel I: Privacy for and from the Digital Person [A National Symposium on Law and Technology]*, The Federalist Society, Oct. 18, 2021, 21:44–22:15, https://www.youtube.com/watch?v=JSvws3PRArE&ab_channel=TheFederalistSociety.

[76] Attorney General Donovan Sues Clearview AI for Violations of Consumer Protection Act and Data Broker Law, Office of the Vermont Attorney General, Mar. 10, 2020, https://ago.vermont.gov/blog/2020/03/10/attorney-general-donovan-sues-clearview-ai-violations-consumer-protection-act-and-data-broker-law, emphasis added.

[77] Paresh Dave & Jeffrey Dastin, *EXCLUSIVE Facial recognition company Clearview AI seeks first big deals, discloses research chief*, Reuters, Feb. 22, 2022, https://www.reuters.com/technology/exclusive-facial-recognition-company-clearview-ai-seeks-first-big-deals-2022-02-22/, emphasis added.

[78] Kashmir Hill & Gabriel J.X. Dance, *Clearview's Facial Recognition App Is Identifying Child Victims of Abuse*, The New York Times, Feb. 10, 2020, https://www.nytimes.com/2020/02/07/business/clearview-facial-recognition-child-sexual-abuse.html.

"Clearview AI's practices are particularly unsavory"

for finding their victims, because **it was the first facial recognition database with millions of children's faces**."[79] While stopping and preventing child trafficking is a critically important area of focus for law enforcement, Clearview AI's flagrant constitutional and statutory violations are not granted the imprimatur of legality merely because there are some downstream positive effects.

If Clearview AI is in fact truly incapable of obtaining consent to use the personal data of minors, the solution is not to continue to allow Clearview AI to flout the law, but to prevent Clearview AI from continuing to violate the rights of California's children. As one judge has rightfully concluded, Clearview AI's argument that "[w]e can't possibly get [the people of Illinois's] permission" does not excuse Clearview AI from complying with the law.[80]

Clearview AI's practices are particularly unsavory in that there is no way for an individual to avoid having their biometric information captured and retained in Clearview AI's database, other than to never have their face appear in a single photo online—even one they did not take or know was being taken. As reported by *Business Insider*: "if 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 AI has snapped a picture of your face, it will create a permanent biometric print of your face to be included in the database."[81] As stated by Kashmir Hill: "'[Clearview AI] may well reveal photos that you didn't realize were on the internet, maybe some photos you didn't want to be there.'"[82]

Furthermore, Clearview AI's technology is not designed in a way that enables it to effectively comply with other provisions of the California Consumer Privacy Act. For

---

[79] Kashmir Hill, *My chilling run-in with a secretive facial-recognition app*, The Telegraph, Sept. 27, 2023, https://www.telegraph.co.uk/books/non-fiction/clearview-ai-facial-recognition-app-chilling/, emphasis added.

[80] See *ACLU*, *supra*, Decision Denying Clearview AI's Motion to Dismiss, pp. 11–12.

[81] Katherine Tangalakis-Lippert, *Clearview AI scraped 30 billion images from Facebook and other social media sites and gave them to cops: it puts everyone into a 'perpetual police line-up'*, Business Insider, Apr. 2, 2023, https://www.businessinsider.com/clearview-scraped-30-billion-images-facebook-police-facial-recogntion-database-2023-4.

[82] See fn. 9.

example, Civil Code section 1798.120, subdivision (d) provides that where a business receives a consumer's request to opt-out of the sale of their personal information, the business "shall be prohibited . . . from selling . . . the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides consent, for the sale . . . of the consumer's personal information." Civil Code section 1798.121, subdivision (b) provides consumers a right to prohibit businesses "from using or disclosing the consumer's sensitive personal information." The problem is that Clearview AI is incapable of complying with such requests because it functions by automatically scraping images off the web without regard for whose images are being scraped or whether the scraped images are of people who have prohibited Clearview AI from using or disclosing their biometric information. As reported in *Wired*: "The way Clearview works—by sending bots to search the internet for faces and then storing them in a database—makes it impossible to keep EU faces from appearing on the platform, according to CEO Hoan Ton-That."[83] Indeed, it is questionable whether Clearview AI is even able to comply with the requirement to delete a consumer's personal information upon request pursuant to Civil Code section 1798.105, with *Wired* noting: "Clearview did not reply to a request to comment on whether it is able to permanently delete people from its database."[84] Thus, one IT security researcher stated he "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."[85]

"The California Privacy Protection Agency should cooperate with the numerous other polities that have already concluded that Clearview AI has violated individuals' privacy rights."

This flagrant and flippant disregard of the law typifies how Clearview AI has conducted itself – as though it were above the law. Its refusal to pay any of the fines imposed or comply with the orders of numerous regulators in the European Union is

[83] Morgan Meaker, *Clearview Stole My Face and the EU Can't Do Anything About It*, Wired, Nov. 7, 2022, https://www.wired.com/story/clearview-face-search-engine-gdpr/.

[84] *Ibid.*

[85] *Ibid.*

another, with *Wired* reporting that "[f]rustration is growing in Europe that face search engines [including Clearview AI] keep operating in blatant defiance of regulators' orders to stop processing EU faces."[86]

The California Privacy Protection Agency is charged with "[c]ooperat[ing] with other agencies with jurisdiction over privacy laws and with data processing authorities in California, other states, territories, and countries to ensure consistent application of privacy protections."[87] The California Privacy Protection Agency should cooperate with the numerous other polities that have already concluded that Clearview AI has violated individuals' privacy rights. Some examples include:

- In February 2021, Canada's privacy commissioner stated bluntly: "'What Clearview does is mass surveillance, and it is illegal,'" and remarked that the company's behavior was "'completely unacceptable.'"[88]

- In November 2021, Australia's Information/Privacy Commissioner "found that Clearview AI, Inc. breached Australians' privacy by scraping their biometric information from the web and disclosing it through a facial recognition tool," and ordered the company to stop processing residents' data and delete such data already collected.[89]

- In December 2021, France's privacy watchdog found that Clearview AI had violated the General Data Protection Regulation ("GDPR")[90], and ordered the company to stop its "'unlawful processing'" of residents' data, and to delete any such data within two months.[91] In October 2022, after Clearview AI failed to respond to the previous order, the watchdog fined Clearview AI €20 million,

---

[86] *Ibid.*

[87] Civ. Code § 1798.199.40, subd. (i).

[88] Kashmir Hill, *Clearview AI's Facial Recognition App Called Illegal in Canada*, The New York Times, Feb. 3, 2021, https://www.nytimes.com/2021/02/03/technology/clearview-ai-illegal-canada.html.

[89] *Clearview AI breached Australians' privacy*, Office of the Australian Information Commissioner, Nov. 3, 2021, https://www.oaic.gov.au/newsroom/clearview-ai-breached-australians-privacy.

[90] See Kukielski, *The First Amendment*, *supra*, 55 Loyola L.A. L.Rev. at pp. 272–73 (noting that the "CCPA and CPRA are the first consumer privacy laws in the country to approximate the comprehensive data privacy laws already found in Europe," and that the "CCPA and CPRA mark a shift towards the more broadly applicable regulatory approach taken in the European Union's" GDPR).

[91] Natasha Lomas, "France latest to slap Clearview AI with order to delete data," TechCrunch, Dec. 16, 2021, at https://techcrunch.com/2021/12/16/clearview-gdpr-breaches-france/.

the maximum amount permitted under the GDPR, for breaches including "[u]nlawful processing of personal data" and "[i]ndividuals' rights not respected," as well as Clearview AI's failure to cooperate with the agency.[92] In May 2023, the watchdog fined Clearview AI an additional €5.2 million for failing to comply with its orders.[93]

- In May 2022, the United Kingdom's data privacy authority fined Clearview AI £7.5 million, and ordered the company to stop processing residents' data and delete any data already collected.[94] The U.K.'s information commissioner remarked: "'The company not only enables identification of those people, but effectively monitors their behaviour and offers it as a commercial service. That is unacceptable.'"[95]

- In May 2022, Italy's data protection agency fined Clearview AI €20 million, the maximum amount permitted under the GDPR, with the agency stating: "'Clearview AI's activity [] violates the freedoms of the data subjects, including the protection of confidentiality and the right not to be discriminated against.'"[96] Clearview AI was ordered to delete all residents' data and cease further processing of residents' facial biometrics.[97]

---

[92] Natasha Lomas, *France fines Clearview AI maximum possible for GDPR breaches*, TechCrunch, Oct. 20, 2022, https://techcrunch.com/2022/10/20/clearview-ai-fined-in-france/.

[93] Natasha Lomas, *Clearview fined again in France for failing to comply with privacy orders*, TechCrunch, May 10, 2023, https://techcrunch.com/2023/05/10/clearview-ai-another-cnil-gspr-fine/.

[94] James Vincent, *Clearview AI ordered to delete facial recognition data belonging to UK residents*, The Verge, May 23, 2022, https://www.theverge.com/2022/5/23/23137603/clearview-ai-ordered-delete-data-uk-residents-ico-fine.

[95] *Ibid.* The fine was later overturned on the sole basis that Clearview AI lacked customers within the U.K. —the "decision underlined that scraping large volumes of publicly available data was an activity to which UK data protection rules could apply." (See Chris Vallance, *Face search company Clearview AI overturns UK privacy fine*, BBC News, Oct. 18, 2023, https://www.bbc.com/news/technology-67133157.) The Information Commissioner is now seeking to appeal this decision on the grounds that "Clearview itself was not processing data for foreign law enforcement purposes and should not be shielded from the scope of UK law on that basis." (Martyn Landi, *ICO seeks permission to appeal against Clearview AI tribunal ruling*, Yahoo! Finance, Nov. 17, 2023, https://uk.finance.yahoo.com/news/ico-seeks-permission-appeal-against-111710906.html.)

[96] Natasha Lomas, *Italy fines Clearview AI €20M and orders data deleted*, TechCrunch, Mar. 9, 2022, https://techcrunch.com/2022/03/09/clearview-italy-gdpr/.

[97] *Ibid.*

- In July 2022, Greece's data protection authority fined Clearview AI €20 million, the maximum amount permitted under the GDPR, and ordered the company to stop collecting and processing residents' data and delete any such data already collected.[98]

Official infographic published by the French data protection authority.

[98] *Hellenic DPA fines Clearview AI 20 million euros*, European Data Protection Board, July 20, 2022, https://edpb.europa.eu/news/national-news/2022/hellenic-dpa-fines-clearview-ai-20-million-euros_en.

VII. Conclusion

Facial recognition technology may have beneficial applications. However, the use of such technology must be conditioned under a strict regulatory system that ensures that common citizens' privacy rights are not being violated, and to ensure that the data that feeds such technology is acquired legally and remains subject to all necessary safeguards and protections. Clearview AI, in contrast, vigorously contests any efforts to regulate its activities, and has shown a willingness and "ability to control not only who law enforcement is able to find using their application, but also [to] manipulate the results of their search."[99] Clearview AI from the start has flagrantly disregarded social and ethical norms that even companies like Google and Facebook refuse to transgress.

Clearview AI is simply not a company that can be trusted with mountains of illegally obtained biometric data. The Office of the Attorney General and the California Privacy Protection Agency should use all the powers available to them to enjoin the use of Clearview AI's facial recognition technology by any public agency or department, and to take all punitive action deemed appropriate in light of Clearview AI's repeated and flagrant violations of law.

[99] Shamhart, *The Mosaic Theory*, *supra*, 51 Cap. U. L. Rev. at p. 527.