Ellen V. Leonida (SBN: 184194)
leonida@braunhagey.com
Matthew Borden, Esq. (SBN: 214323)
borden@braunhagey.com
J. Noah Hagey, Esq. (SBN: 262331)
hagey@braunhagey.com
Athul K. Acharya (SBN: 315923)
acharya@braunhagey.com
Gunnar K. Martz (SBN: 300852)
martz@braunhagey.com
BRAUNHAGEY & BORDEN LLP
351 California Street, Tenth Floor
San Francisco, CA 94104
Telephone: (415) 599-0210
Facsimile: (415) 276-1808

Sejal R. Zota (*pro hac vice* application forthcoming)
sejal@justfutureslaw.org
Dinesh McCoy (*pro hac vice* application forthcoming)
dinesh@justfutureslaw.org
JUST FUTURES LAW
95 Washington Street, Suite 104-149
Canton, MA 02021
Telephone: (919) 698-5015

Attorneys for PLAINTIFFS STEVEN RENDEROS, VALERIA THAIS SUÁREZ ROJAS, REYNA MALDONADO, LISA KNOX, MIJENTE SUPPORT COMMITTEE, and NORCAL RESIST FUND

SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF ALAMEDA

STEVEN RENDEROS, VALERIA THAIS SUÁREZ ROJAS, REYNA MALDONADO, LISA KNOX, MIJENTE SUPPORT COMMITTEE, and NORCAL RESIST FUND,

Plaintiffs,

v.

CLEARVIEW AI, INC., and DOES 1-10,

Defendants.

Case No. _____

COMPLAINT

Plaintiffs Steven Renderos, Valeria Thais Suárez Rojas, Reyna Maldonado, Lisa Knox, Mijente Support Committee, and NorCal Resist Fund allege as follows:

INTRODUCTION

1. Plaintiffs are two community-based organizations and four political activists. They bring this action under California law to enjoin Defendant Clearview AI, Inc. ("Clearview") from illegally acquiring, storing, and selling their likenesses, and the likenesses of millions of Californians, in its quest to create a cyber surveillance state.

2. Defendant Clearview is a company with ties to alt-right and white supremacist organizations. 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 times the size of the FBI's. Clearview has provided thousands of governments, government agencies, and private entities access to its database, which they can use to identify people with dissident views, monitor their associations, and track their speech. As expressly intended by Clearview's creators and early investors, its mass surveillance technology disproportionately harms immigrants and communities of color.

3. Clearview built its database by violating the privacy rights of Plaintiffs and all California residents and making commercial use of their likenesses. Clearview illicitly gathers, copies, and saves images by "scraping" them from websites, like Facebook, Twitter, and Venmo. Clearview persists despite having received multiple requests to stop this practice, which violates many of the websites' terms of service and the contracts between the sites and their users.

4. After obtaining these images, Clearview uses algorithms to extract the unique facial geometry of each individual depicted in the images, creating a purported "faceprint" that serves as a key for recognizing that individual in other images, even in photographs taken from different angles. Clearview's "faceprints" rely on an individual's immutable biological characteristics—for example, the position, size, and shape of the eyes, nose, cheekbones, and jaw—to purportedly capture their biometric signature.

5. Clearview's end product is facial recognition technology that claims to enable its users to identify virtually anyone simply by uploading a photograph. Users can photograph a

stranger at a political rally or house of worship, upload the photo to Clearview's database, and instantly see other photographs of the same person linked to various social media platforms and websites. The websites often describe the person's address, employment information, political affiliations, religious activities, and familial and social relationships, among other sensitive information. With Clearview, users can access all this information on their phones with the tap of a finger. Clearview's portable surveillance technology thus provides instantaneous access to almost every aspect of our digital lives.

6. Clearview has licensed its database to governments around the world, large-scale retailers, and law enforcement agencies throughout the United States. According to news reports, by February 2020, people associated with 2,228 companies, law enforcement agencies, and other institutions had collectively performed nearly 500,000 searches of Clearview's faceprint database. In August 2020, Clearview's CEO bragged that over 2,400 police agencies were using Clearview.

7. Clearview has been banned internationally. Canada has asked Clearview to remove the faces of Canadian residents from its database, because "what Clearview does is mass surveillance"—putting all Canadians "continually in a police lineup."[1] Similarly, the European Union recently found, after an 11-month investigation, that Clearview's practices violate its General Data Protection Regulations.

8. Multiple municipalities and law enforcement agencies in the United States have also banned Clearview and other facial recognition technology, in part because of the potential for abuse, false positives, and image manipulation. Studies have found empirical evidence of racial, gender, and age bias in facial recognition technology—with Asians and African Americans 100 times more likely to be misidentified than white men.

9. Nonetheless, Clearview continues to sell access to its database to California police agencies and U.S. Immigration and Customs Enforcement (ICE). This is not happenstance; one person who helped build Clearview stated in 2017 that the purpose of the technology was to "ID all the illegal immigrants for the deportation squads." ICE can deploy Clearview's technology even in

[1] Kashmir Hill, *Clearview AI's Facial Recognition App Called Illegal in Canada,* N.Y. TIMES, (Feb. 3, 2021), https://www.nytimes.com/2021/02/03/technology/clearview-ai-illegal-canada.html

cities and counties that have banned the use of facial recognition technology, as have multiple cities in Alameda County.

10. Plaintiffs are activists, including immigrants, who have engaged in political speech critical of the police, ICE, and immigration policy in both their personal and professional capacities. Plaintiffs Mijente Support Committee ("Mijente") and NorCal Resist Fund ("NorCal Resist") are two immigrant rights, membership-based organizations representing the interests of thousands of California residents. The ability to control their likenesses and biometric identifiers—and to continue to engage in political speech critical of the police and immigration policy, free from the threat of clandestine and invasive surveillance—is vital to Plaintiffs, their members, and their missions.

PARTIES

A. Plaintiffs

11. Plaintiff Steven Renderos ("Plaintiff Renderos") is a resident of Alameda County and the Executive Director of the Center for Media Justice, a grassroots organization fighting for racial, economic, and gender justice in a digital age. The Center for Media Justice has recently focused on challenging the use of invasive technology in the context of policing and the criminal legal system, as well as ensuring that people of color have the communications tools to amplify their voices effectively. Plaintiff Renderos has worked with the Center for Media Justice for almost nine years, and his role includes developing strategy for Media Justice's programmatic work. Plaintiff Renderos frequently uses social media for both personal and professional purposes and has public-facing Facebook and Twitter accounts where he frequently expresses his views for the purposes of political and policy advocacy. Plaintiff Renderos is frequently critical of police and ICE practices in both his personal and professional capacity, and he has been a public advocate on the importance of limiting the use of surveillance technology by law enforcement. On information and belief, Clearview has captured Plaintiff Renderos' biometric data and stored it in its faceprint database. Plaintiff Renderos has never consented to having Clearview collect or use his image or biometric data.

12. Plaintiff Valeria Thais Suárez Rojas ("Plaintiff Suárez") is a resident of Alameda County and formerly worked as the Bay Area Youth Coordinator at California Immigrant Youth Justice Alliance (CIYJA), where she was a vocal advocate on behalf of immigrant rights. She continues to work on immigrant rights issues in the Bay Area. Plaintiff Suárez is an immigrant herself, and has engaged in political speech critical of the police, ICE, immigration policy, and other government entities. Plaintiff Suárez has uploaded photos of herself on several social media platforms including Twitter, Instagram, Facebook, and Venmo. She has included pictures of herself with her friends and family on these platforms, and her friends and family have also posted pictures including Plaintiff Suárez. She frequently uses her social media accounts as activism tools, and posts content related to her political views on these platforms. Specifically, Plaintiff Suárez has used her social media accounts to criticize ICE and raise money for community members recently released from detention, among other political and organizing-based messages. Plaintiff Suárez made her social media accounts private in early 2020. While she occasionally makes her accounts public to support fundraising campaigns, they usually remain private. However, others have continued to post photos of her on social media platforms. On information and belief, Clearview has captured her biometric data and stored it in its faceprint database, including images of her face that are no longer publicly accessible. Plaintiff Suárez has never consented to Clearview collecting or using her image or her biometric data.

13. Plaintiff Lisa Knox ("Plaintiff Knox") is a resident of Alameda County and Legal Director of the California Collaborative for Immigrant Justice, where she works to create and support strategies to fight for the liberation of immigrants in detention through direct representation, litigation, and advocacy. Previously, Plaintiff Knox was a managing attorney at Centro Legal de la Raza, where she helped found and manage the detained representation project. Plaintiff Knox oversaw emergency legal services for Alameda County's rapid response network and managed legal clinics at two California detention centers. Plaintiff Knox participates in and often speaks at demonstrations critical of ICE and the police. Plaintiff Knox has used several social media platforms including Twitter, Instagram, Facebook, and Venmo, and she has uploaded photos of herself, including photographs of herself with friends and family, on these platforms. Plaintiff

Knox frequently uses her social media accounts as activism tools and has posted content critical of police and ICE. On information and belief, Clearview has captured her biometric data and stored it in its faceprint database. Plaintiff Knox has never consented to Clearview collecting or using her image or biometric data.

14. Plaintiff Reyna Maldonado ("Plaintiff Maldonado") is currently a business owner in, and resident of, Oakland, California. Plaintiff Maldonado formerly worked as an immigrant rights community organizer. Plaintiff Maldonado is an immigrant who has deferred action as a result of the Deferred Action for Childhood Arrivals (DACA) program. As an organizer, she worked in coalitions to support undocumented youth in the Bay Area, including by supporting housing and employment efforts and by promoting mental health resources for undocumented organizers. Plaintiff Maldonado frequently uses social media both for personal and business purposes. Plaintiff Maldonado currently owns a restaurant, and uses social media to help advertise the business and share updates with customers. While her personal accounts are private, she has at times loosened the privacy restrictions. Plaintiff Maldonado has used these accounts as an activism tool, posting about political issues related to immigrant rights advocacy, posting in support of the Black Lives Matter movement, and speaking out against police and ICE practices. On information and belief, Clearview has captured her biometric data and stored it in its faceprint database. Plaintiff Maldonado has never consented to Clearview collecting or using her image or biometric data.

15. Plaintiff NorCal Resist, a California corporation, is a grassroots, membership-based organization working to equip impacted communities with the tools needed to fight immigration injustice. Plaintiff NorCal Resist has a significant interest in ensuring that immigrant and activists' rights are respected and upheld, including their rights to safety and privacy. Plaintiff NorCal Resist hosts Know Your Rights trainings relating to direct actions and navigating encounters with ICE and police, assists with rapid response to support local residents targeted in immigration enforcement actions, and has a bail fund that supports community members arrested in racial justice protests or for immigration-related charges. Plaintiff NorCal Resist has close to 7,000 members throughout Northern California, including more than 200 members in Alameda County. Members support the organization by donating money and volunteering to support local actions and events, and members

vote on the leadership of the organization. NorCal Resist members have been critical of ICE, immigration policy, and policing tactics, and they have expressed concern through both their conduct and speech in relation to their work with Plaintiff NorCal Resist. On information and belief, the biometric information and identifiers of many members of Plaintiff NorCal Resist have been, and will continue to be, captured in Clearview's database without their consent. Clearview's practices pose a threat to Plaintiff NorCal Resist's members by divesting them of the power to control their biometric identifiers, and by chilling their ability to exercise various constitutional rights—including the right to protest and to travel—without being instantaneously identified and tracked.

16. Plaintiff Mijente, an Arizona corporation, is a national digital and grassroots hub for Latinx and Chicanx movement building and organizing that seeks to increase the profile of policy issues that matter to its communities and increase the participation of Latinx and Chicanx people in the broader movements for racial, economic, climate, and gender justice. Plaintiff Mijente organizes around surveillance issues in the immigrant community, particularly in the face of increasing technological capabilities of corporations and the government, and has a significant interest in halting data sharing practices that result in the arrest, detention, and deportation of immigrants. Mijente has more than 300 members in California and 50 in Alameda County, many of whom have, at times, uploaded their photos to various internet-based platforms and websites, and have engaged in political speech that could be considered critical of the police, ICE, immigration policy, and other government entities. Plaintiff Mijente's members have specifically criticized law enforcement's use of surveillance technology to police immigrant communities. These members use their accounts as an activism tool, and on information and belief, their biometric information and identifiers have been, and will continue to be, captured in Clearview's database without their consent. Clearview's practices pose a threat to Plaintiff Mijente's members by divesting them of the power to control their biometric identifiers, and by chilling their ability to exercise various constitutional rights—including the right to protest and to travel—without being instantaneously identified and tracked.

17. Plaintiffs Suárez, Knox, Maldonado, and Renderos, as well as members of Plaintiffs NorCal Resist and Mijente, did not consent to have their biometric data harvested by Clearview, did not understand that their biometric data could or would be obtained by Clearview or anyone else when they posted images of themselves and their friends, families and associates, and have suffered multiple injuries as a result of Clearview's actions, including, without limitation: expenditure of resources in understanding the extent of Clearview's misappropriation of their and their members' identities, images, likenesses, and biometric data; loss of their property rights in their own identities, images, likenesses, and biometric data; mental anguish as a result of the invasion of their privacy; and fear that they and their communities and families will be targeted for their political speech, associations, affiliations, and/or immigration status.

B. Defendant

18. Defendant Clearview AI, Inc., is a Delaware corporation with its principal place of business in New York, NY. Clearview conducts business throughout the State of California. On information and belief, Clearview was founded by Hoan Ton-That (far right, below) and Richard Schwartz, a former aide to Rudy Giuliani, Esq.

19. Clearview founder Hoan Ton-That, as well as several people associated with Clearview, have a history of longstanding ties to the alt-right, a far-right ideology based on the belief that white identity is under attack. Persons with ties to Clearview include "pizzagate" conspiracy theorist Mike Cernovich; neo-Nazi hacker and *The Daily Stormer* webmaster, Andrew Auernheimer; former chief technology officer of Business Insider who marched with neo-Nazis in

Charlottesville, Virginia, Pax Dickinson; and former Breitbart writer Charles Johnson. In a Facebook post, Johnson described "building algorithms to ID all the illegal immigrants for the deportation squad," likely referring to Smartcheckr, Defendant's name before being rebranded to "Clearview." Marko Jukic is a former Clearview employee whose job included pitching Clearview to law enforcement agencies. In 2015, he wrote that he "wholeheartedly endorse[s] racism, racialism, ethnocentrism, Islamophobia, Eurocentrism and anti-Semitism." Writing under a pseudonym, Jukic described diversity and equality as "indisputably corrosive to civilization," and that "violence most definitely is the answer."

20. Clearview has registered as a data broker in the State of California. It has sold licenses to policing agencies such as the El Segundo and Antioch Police Departments. It promotes and markets its faceprint database throughout the State of California, in part by offering trial use. The Los Angeles Police Department, Long Beach Police Department, San Diego Police Department, San Diego District Attorney's Office, Orange County Sheriff's Office, and San Mateo Sheriff's Office have all used Clearview on a trial basis. Additionally, Clearview engages in the widespread collection of California residents' images and biometric information without notice or consent. On information and belief, Clearview illicitly scrapes images of thousands of people from websites and platforms owned and operated by California-based companies, such as Facebook.

21. Does 1-10 are individuals who have participated in, and/or aided and abetted Clearview in the unlawful acts set forth herein.

JURISDICTION AND VENUE

22. The Court has personal jurisdiction over Clearview pursuant to California Code of Civil Procedure § 410.10 because Clearview conducts business transactions in California; has intentionally availed itself of the laws and markets of California through the use, promotion, sale, and marketing, and/or distribution of its products and services at issue in this Complaint; unlawfully acquires and profits from the biometric data of California residents; has committed unlawful acts arising from and related to its conduct and activity in California complained of in this complaint; and has committed unlawful acts expressly aimed at California residents from which this action arises.

23. Venue is proper in Alameda County pursuant to California Code of Civil Procedure § 395.5 because Plaintiffs' injuries occurred in Alameda County and Defendant Clearview is a foreign corporation within the meaning of California Corporations Code § 171 but has not registered a principal place of business with the California Secretary of State.

FACTUAL ALLEGATIONS

I. DEFENDANT CLEARVIEW'S FACIAL RECOGNITION TECHNOLOGY

A. How Clearview Constructs Its Illegal Database

24. To build its database, Clearview illicitly scrapes images of millions of people from hundreds of websites including Facebook, Twitter, LinkedIn, Venmo, employment sites, and news sites. Scraping is the process of using automated computer software to gather and copy data from websites on the internet into a database for further retrieval and analysis. To date, Clearview purportedly has scraped more than three billion images of human faces, which the company then stores in its database.

25. At no point does Clearview attempt to inform the individuals whose likenesses Clearview acquires that Clearview is collecting and gathering their images. It does not obtain those individuals' consent. Clearview also does not notify individuals that it may be breaching websites' terms of service to scrape, store, and use the individuals' images. Nor does Clearview seek their consent to do so.

26. Clearview also scrapes images of people that were uploaded without their knowledge or consent, including images posted by friends or relatives and even images of people who inadvertently appear in the backgrounds of photographs taken by strangers. In those instances, the individual consents neither to having her image uploaded nor to Clearview scraping and using the image.

27. Multiple online entities, including Google, YouTube, Facebook, Venmo, LinkedIn, and Twitter, have requested that Clearview cease and desist scraping images from their platforms. These companies determined that Clearview's scraping was so invasive that it violated their terms of service with their respective users. Therefore, even if a user consents to a website's terms of service, that consent does not extend to Clearview's scraping.

28. After scraping the data, Clearview extracts biometric information—the distinct and immutable physical characteristics of an individual that can be used to later identify that individual—from the scraped images. A biometric identifier is a piece of biometric information that Clearview can use to authenticate an individual's identity. Clearview extracts biometric identifiers based on individuals' faces, such as the position, size, and shape of the eyes, nose, cheekbones, and jaw.

29. Clearview uses artificial intelligence ("AI") technology to analyze the facial geometry of the faces contained within the scraped images. During the analysis step, Clearview uses its facial recognition AI's analysis of scraped images to create faceprints, which are digitally recorded representations of individuals' faces. Clearview uses individuals' biometric data to create faceprints; faceprints are not accessible or perceptible without Clearview's technology.

30. During the recognition step, Clearview uses its facial recognition AI to search, identify, classify, and index faceprints in its database.

31. Clearview created a mobile application that allows its users to have access to Clearview's database of images. Users may upload a photo, known as a "probe image," to the mobile application, and Clearview's facial recognition software will match the uploaded photo to faceprints within the database. It will display the faceprints, as well as links to the web pages from which Clearview obtained the photographs to capture those faceprints. Those websites often describe sensitive personal information including address, employment, relationship, and political opinion information, furthering the privacy harms. Because Clearview has scraped those images, they are available in Clearview's database even if the image no longer exists on the original website.

32. In addition to scraped images, Clearview retains the probe images the user uploaded to search its database. By default, Clearview stores the probe images on its servers "forever."

33. Clearview maintains a log of all searches ever conducted in its database by anyone. Clearview also appears to monitor searches clients run on its database. After a reporter asked police officers to upload a probe image of her into Clearview's database, for example, the company told the officers that they should not be speaking to the media.

34. Because Clearview extracts biometric information from images, its database contains physical characteristics of individuals. Individuals can change their characteristics only through extreme means like plastic surgery. Therefore, once Clearview enters an individual into its database, that individual permanently loses anonymity and privacy. Indeed, Clearview allows anyone with access to its database to capture a single photo of an individual, and with a few keystrokes, to determine the identity of the person and their personal details in real time—as they shop in the grocery store, attend a political rally, or walk down the street. Clearview has repeatedly touted its ability to provide information about people in "real-time" in patent applications.

35. Facial recognition algorithms have repeatedly been shown to perform poorly when examining the faces of people of color. Consequently, facial recognition technology has a far greater risk of misidentifying people of color. Multiple municipalities, including San Francisco and Oakland, have rejected facial recognition technology for that very reason. For example, a recent study by the National Institute of Standards and Technology (NIST) found that a majority of facial surveillance software exhibits racial bias.[2] According to that study, African American and Asian people are up to 100 times more likely to be misidentified by a facial recognition system than white men, depending on the algorithm and use case.[3] Clearview has refused to participate in NIST's Facial Recognition Vendor Test Program or any other meaningful, independent review.

B. Who Can Access Clearview

36. By February 2020, Clearview had shared its technology with more than 2,200 law enforcement departments, government agencies, and private companies across 27 countries.

37. Of particular concern, the Clearview database allows law enforcement agencies not only to identify people in public spaces, but also to learn those people's professional roles,

---

[2] Patrick Grother, Mei Ngan, & Kayee Hanaoka, Nat'l Inst. of Standards and Tech., U.S. Dep't of Commerce, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NISTIR 8280 (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[3] These "demographic differentials" in error rates are severe enough that in 2019, members of Congress called on the Trump administration to reconsider its plans to expand the use of facial recognition technology. *See* Drew Harwell, *Federal Study Confirms Racial Bias of Many Facial-Recognition Systems, Casts Doubt on Their Expanding Use*, Washington Post (Dec. 19, 2019), https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/.

religious affiliations, familial connections and friendships, romantic partnerships, personal activities, political views, patterns of travel, and even home addresses, all without receiving consent, obtaining a warrant, or providing probable cause to conduct a search.

38. Clearview has selectively provided access to its database to its friends and investors. For example, John Catsimatidis, the billionaire owner of the Gristedes grocery store chain, used the technology to identify and investigate his daughter's boyfriend.

39. Clearview's collection of faceprints also poses an inherent security risk, as this sensitive information may be subject to hacking and data breaches. Breaches of biometric data are particularly harmful since, as noted above, biometrics cannot readily be changed. Once someone's biometric information has been compromised, there is no redress.

40. Clearview has a history of data breaches. In February 2020, hackers gained access to Clearview's client list. Clearview responded to the breach by stating that "data breaches are part of life in the 21st Century."

41. In addition, in early 2020, cybersecurity firm SpiderSilk discovered a misconfigured server which allowed it to access Clearview's source code, applications, and internal files, including 70,000 videos taken from one of Clearview's prototype Insight Cameras located in the lobby of a residential building.

42. In response, Clearview's CEO stated that Clearview experiences "a constant stream of cyber intrusion attempts, and [that Clearview had] been investing heavily in augmenting our security." This blasé attitude is emblematic of Clearview's response to its significant security vulnerabilities. On information and belief, Clearview has taken no concrete measures to shore up its data security, even though the sheer size of its database makes it a tempting target for hackers and risks exposing people's immutable data and personal information.

II. POLICE AND IMMIGRATION ENFORCEMENT AGENCIES USE CLEARVIEW

43. According to Clearview, over 2,400 law enforcement agencies at both the federal and the state level have used its technology since January 2019.

44. Further, one of Clearview's main marketing strategies is to offer free trials to police agencies. Clearview has promoted free trials to several police agencies across California including

Orange County Sheriff's Department, Fresno Police Department, Santa Monica Police Department, Long Beach Police Department, Los Angeles Police Department, and San Diego Police Department, and several of these agencies have accepted its offer.

45. Clearview's marketing materials tout "unlimited searches" and encourage officers not to "stop at one search." They also suggest that officers "search a celebrity to see how powerful the technology can be."

46. Clearview also offers its users the ability to map subjects' associational networks. For example, if a search is run on Person A, the results could include a photograph of Person A with other people, including Person B. The user can then click on the face of Person B and immediately run her through the database. In this way, Clearview compromises Plaintiffs' associational privacy as well.

47. In June 2019, ICE began a paid pilot program with Clearview without a formal contract. The units of the Department of Homeland Security ("DHS") initiating searches included Customs and Border Patrol ("CBP") and ICE Enforcement and Removal Operations ("ERO"). ERO is the body responsible for the arrest and deportation of noncitizens present in the United States without status.

48. On August 12, 2020, Clearview entered into a purchase order contract in which ICE agreed to pay $224,000 for "clearview licenses."

49. Plaintiffs' concerns about being targeted and misidentified are not abstract—ICE has a history of collection of biometric data to use against vulnerable populations. Since 2015, for example, ICE has performed thousands of faceprint searches on state DMV databases, unbeknownst to license holders, to identify, locate, and deport individuals. ICE has conducted these searches in at least three states that allow undocumented immigrants to obtain a license or driver privilege card. ICE runs these searches without a warrant or any other official approval.

50. Plaintiffs' concerns are heightened in light of ICE's history, including its recent role in family separation, its longstanding practice of detaining people in horrific conditions, and its pattern of racial and religious profiling. ICE has also systematically surveilled, detained, and deported immigrant activists who speak out about immigration policies and practices. For example,

ICE has targeted Maru Mora-Villalpando, a member of both La Resistencia and Mijente, because of her "anti-ICE protests." Ravi Ragbir was arrested, at his ICE check-in meeting, after protests that ICE characterized as an unwanted "display of wailing kids and wailing clergy." Daniela Vargas was arrested as she left a press conference supporting the DACA program. A number of immigrant rights groups and immigrants have sued ICE for violating their rights to speak, assemble, and associate under the First Amendment.

51. Federal agencies, including DHS and its subsidiaries, also have a history of conducting intrusive surveillance on protestors associated with the Black Lives Matter movement. A leaked memorandum shows that the Department of Justice ("DOJ") authorized the Drug Enforcement Administration to "conduct covert surveillance" and collect intelligence on people participating in protests over the police killing of George Floyd. In summer 2020, DHS units deployed agents to protests associated with the Black Lives Matter movement across the United States. CBP agents detained protestors, abducting them from the streets of Portland despite a lack of probable cause. Additionally, in May 2020, CBP deployed a Predator drone over Black Lives Matter protestors in Minneapolis. The drone "was preparing to provide live video to aid in situational awareness at the request of our federal law enforcement partners in Minneapolis."

52. Law enforcement has deployed Clearview's facial recognition technology to identify and arrest demonstrators exercising their First Amendment rights at a protest in Miami. Reports indicate that Minnesota law enforcement may have been using Clearview's facial recognition technology on protestors, particularly in Minneapolis, which prompted Senator Edward Markey of Massachusetts to write to Clearview "to take urgent action to prevent the harmful use of its product."

53. Senator Markey also wrote to former Attorney General William Barr, expressing concern about the DOJ's surveillance of Black Lives Matter protesters and potential use of Clearview as part of that surveillance.[4]

[4] Letter from Senator Edward J. Markey to Attorney General William Barr (June 11, 2020), https://www.markey.senate.gov/imo/media/doc/DOJ%20Protest%20Surveillance.pdf.

54. In response to the Black Lives Matter protests in the summer of 2020 and concerns over law enforcement's misuse of facial recognition technology—and the potential racial bias inherent in that technology—several companies making facial recognition software, including IBM and Amazon, decided to pause or halt selling their software to law enforcement. Clearview's CEO stated that Clearview would continue to sell its technology to law enforcement despite these concerns.

55. Clearview's partnership with ICE poses a grave threat to First Amendment rights and chills Plaintiffs and others from participating in constitutionally protected activity. ICE can deploy Clearview throughout California, including Alameda County, where multiple communities have banned local law enforcement's use of facial recognition technology.

56. Clearview allows ICE to conduct arbitrary digital searches of Plaintiffs, their members, and other California residents, instantly accessing their faceprints without privacy safeguards, warrants, or a showing of reasonableness. Given ICE's record of conducting intrusive surveillance on immigrant communities and protestors, Plaintiffs fear that ICE will use Clearview's faceprint database to surveil and target their communities, exacerbating their injury.

57. Plaintiffs also fear that the potential racial bias inherent in the technology will increase the risk of misidentification by ICE and police officers.

III. CLEARVIEW VIOLATES PLAINTIFFS' RIGHTS

58. On information and belief, Clearview has scraped (and continues to scrape) images of Plaintiffs Renderos, Suárez, Knox, and Maldonado from websites, extracted the biometric data from the individual Plaintiffs' images, calculated their unique physical characteristics, and generated a faceprint biometric template therefrom enabling the identification of Plaintiffs, in direct violation of the laws identified in this Complaint, and without notice to, or permission from, Plaintiffs.

59. Clearview sells access to its database containing the individual Plaintiffs' images and faceprints to third-party entities for commercial monetary gain. Clearview does so without permission or notice.

60. Plaintiffs Mijente and NorCal Resist's members, like millions of other California residents, have uploaded numerous photos of themselves to social media sites and other websites. Others have uploaded photos of them as well. Upon information and belief, Clearview has captured the faceprints of members of Plaintiffs NorCal Resist and Mijente from photographs online. The sheer volume of online photographs Clearview scrapes to capture faceprints for its database makes it a near certainty that anyone whose photographs are posted to publicly accessible portions of the internet will have been subjected to surreptitious and nonconsensual faceprinting by Clearview.

61. For example, Confidential Member 1 is a resident of Alameda County and an active member of NorCal Resist. Confidential Member 1 regularly engages in speech that is critical of both police and ICE by participating in demonstrations. At those events, because of concerns for his security and fear of surveillance, he often wears a mask. Confidential Member 1 is active on Facebook, where he has a private account (but a publicly accessible profile page on which his photo sometimes appears). He shares commentary there, also, that could be viewed as critical of law enforcement. On information and belief, Clearview has captured his images, extracted his biometric information, and converted them into faceprints for Clearview's faceprint database. Confidential Member 1 has never given Clearview consent to do so. Learning that he is in the database where he can be identified has caused him to suffer mental anguish.

62. Similarly, Confidential Member 2 is a resident of Alameda County and an active member of Mijente. Confidential Member 2 regularly criticizes ICE and police practices, and engages in numerous organizing efforts around the Bay Area to promote immigrant rights. Confidential Member 2 is active on Facebook and Twitter, and frequently posts content critical of immigration enforcement policies. His Facebook account is private, and he removed his name and face image from Twitter in early 2021 because of concerns about his privacy and potential use of his images without his consent. On information and belief, Clearview has captured his images, extracted his biometric information, and converted them into faceprints for Clearview's faceprint database. Confidential Member 2 has never given Clearview consent to do so. Learning that he is in the database where he can be identified has caused him to suffer mental anguish.

63. Through its unauthorized access, use, and sale of Plaintiffs' photographs and biometric data, Clearview infringes on Plaintiffs' interests in data security and ownership and control of their identities, likenesses, personal data, and biometric identifiers.

64. Furthermore, because Clearview sells its faceprint database to hundreds of law enforcement entities, Plaintiffs have suffered injury to their peace of mind arising from their fear that they will be retaliated against for their constitutionally protected views regarding policing and immigration. They fear surveillance of their immigrant and people of color communities, and they fear being targeted for arrest and deportation.

65. Plaintiffs Suárez, Knox, Maldonado, and Renderos, as well as members of Plaintiffs NorCal Resist and Mijente, have suffered multiple injuries as a result of Clearview's actions, including, without limitation, that: (1) Plaintiffs have expended resources in an attempt to understand the extent of Clearview's collection of their personal information; (2) Plaintiffs have suffered loss and diminution of their property rights in their own identities, images, likenesses, and biometric data; and (3) Plaintiffs have suffered mental anguish as a result of the invasion of their privacy and worry that they and their communities will be targeted for their political speech or immigration status and misidentified by Clearview's system.

66. There is also a substantial likelihood that Clearview will capture individual Plaintiffs' and organizational Plaintiffs' members' faceprints in the future. The sheer volume of photos ingested by Clearview's technology on an ongoing basis creates a substantial likelihood that any photos newly uploaded to publicly available websites will be obtained by Clearview and used to capture faceprints.

67. Each day that Clearview is allowed to continue its illegal activities, Plaintiffs suffer immediate and irreparable injuries, including chilling of their core First Amendment rights of association and to engage in political speech, injuries to their rights to privacy, injuries to their property rights in their own likenesses and biometric information, and injuries to their peace of mind and wellbeing.

68. Defendants are guilty of recklessness, oppression, fraud, or malice. Defendants' conduct was intended to cause injury to Plaintiffs, and carried out with a willful and conscious disregard of Plaintiffs' rights.

FIRST CAUSE OF ACTION
Common Law Appropriation of Likeness

69. Plaintiffs incorporate all preceding paragraphs as though set forth herein.

70. Under California common law, the right against appropriation of likeness has four elements: "(1) the defendant's use of the plaintiff's identity; (2) the appropriation of plaintiff's name or likeness to defendant's advantage, commercially or otherwise; (3) lack of consent; and (4) resulting injury." *Eastwood v. Superior Court*, 149 Cal. App. 3d 409, 418 (1983).

71. Without providing notice to or obtaining consent from Plaintiffs and Plaintiffs' members, Clearview knowingly and surreptitiously collected Plaintiffs' and Plaintiffs' members' names, photographs, biometric information, and other identifiers (which constitute Plaintiffs' and Plaintiffs' members' "identities") by scraping images from websites in violation of many of the websites' policies prohibiting such conduct.

72. Without notice to or consent from Plaintiffs and Plaintiffs' members, Clearview used their names, photographs, biometric information, and other identifiers to its advantage by copying them, saving them, and selling access to them to private and government entities worldwide.

73. As a direct and proximate result of Clearview's conduct, Clearview has caused Plaintiffs economic injury and mental anguish. By appropriating Plaintiffs' and Plaintiffs' members' identities without consent, Clearview has deprived them of the opportunity to profit by licensing such use. Clearview's nonconsensual and knowing use of Plaintiffs' and Plaintiffs' members' identities for the purpose of commercial profit exposed Plaintiffs to secondary harms related to the sale of Plaintiffs' information to third parties, including law enforcement entities, that chills Plaintiffs' speech. Defendant's sale of Plaintiffs' converted identities has caused Plaintiffs to experience anxiety related to the threat of surveillance by third-party entities, such as ICE.

74. Defendant's conduct has directly and proximately caused loss to Plaintiffs in an amount to be proven at trial. Plaintiffs also seek injunctive and equitable relief as is necessary to protect themselves and other California residents by requiring Clearview to comply with the common-law requirements for the nonconsensual appropriation of Plaintiffs' identities to Defendant's advantage.

SECOND CAUSE OF ACTION
California Constitution art. 1, § 1

75. Plaintiffs incorporate all preceding paragraphs as though set forth herein.

76. Under the California Constitution, art. 1, § 1, "[a]ll people" have certain "inalienable rights," including the right to "pursu[e] and obtain[] . . . privacy." This provision creates a right against private as well as government entities. The elements of this right of action are: (1) a legally protected interest in either "informational privacy" or "autonomy privacy"; (2) a reasonable expectation of privacy; and (3) a serious invasion of the privacy interest.

77. Plaintiffs and Plaintiffs' members have legally protected interests in preventing unwanted access to their data by electronic or other covert means in violation of the law or social norms, in conducting personal activities without observation, and in advance notice and the opportunity to provide or withhold consent to such intrusions. These are all legally protected interests in informational privacy.

78. Plaintiffs and Plaintiffs' members also have legally protected interests in their associational privacy, which is a component of both informational and autonomy privacy.

79. Plaintiffs and Plaintiffs' members have a reasonable expectation of privacy in their names, photographs, biometric information, and other identifiers, because the websites from which Clearview scrapes such information prohibit such conduct in their terms of service. Plaintiffs and Plaintiffs' members also have a reasonable expectation of privacy in their biometric information because it can be used to identify them based on their unique and immutable physical and biological characteristics.

80. Clearview's invasion of Plaintiffs' and Plaintiffs' members' privacy is serious and highly offensive for three reasons: first, because Clearview's conduct is surreptitious, in violation

of websites' terms of service, and in violation of numerous cease-and-desist letters from such websites; second, because 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; and third, 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.

THIRD CAUSE OF ACTION

Business & Professions Code §§ 17200, *et seq*.

81. Individual Plaintiffs incorporate all preceding paragraphs as though set forth herein.

82. The Unfair Competition Law ("UCL") prohibits, *inter alia*, any unlawful or unfair business practice. Clearview's conduct is both unlawful and unfair because it violates California Constitution art. 1, § 1, California Penal Code § 502, California's common-law right against appropriation of likeness, and the terms of use of the various websites where Clearview scraped the data.

83. Individual Plaintiffs lost money or property as a result of Clearview's wrongful conduct. California law recognizes that individuals have a property right in their identity, image, biometric information and likeness, both by statute, Civ. Code §§ 3344, 3344.1, and through its common law appropriation-of-likeness tort. Clearview's use of Individual Plaintiffs' likenesses is a primary factor in private and government entities' purchases of Clearview's services. Without the likenesses of Individual Plaintiffs and others, Clearview would have no service to sell. By appropriating Individual Plaintiffs' likenesses without consent, Clearview has deprived them of the opportunity to profit by licensing such use. Additionally, Individual Plaintiffs have expended resources in understanding the extent of Clearview's misappropriation of their identities, images, likenesses, and biometric data.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully pray for the following:

A. Injunctive relief;

B. Compensatory damages;

C. Exemplary damages;

D. An award of attorney's fees and costs;

E. Any other relief as equity and justice may require.

Dated: March 8, 2021

Respectfully submitted,

Ellen V. Leonida

BRAUNHAGEY & BORDEN LLP

Sejal R. Zota

JUST FUTURES LAW

Attorneys for Plaintiffs Steven Renderos, Valeria Thais Suárez Rojas, Reyna Maldonado, Lisa Knox, Mijente, and Norcal Resist

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial of all claims and causes of action triable before a jury.

Dated: March 8, 2021

Respectfully submitted,

Ellen V. Leonida

BRAUNHAGEY & BORDEN LLP

Sejal Zota

JUST FUTURES LAW

Attorneys for Plaintiffs Mijente, Norcal Resist, Valeria Thais Suárez Rojas, Reyna Maldonado, Lisa Knox, and Steven Renderos