

1 **BRAUNHAGEY & BORDEN LLP**

2 Ellen V. Leonida (SBN: 184194)
3 leonida@braunhagey.com
4 Matthew Borden (SBN: 214323)
5 borden@braunhagey.com
6 J. Noah Hagey (SBN: 262331)
7 hagey@braunhagey.com
8 Tracy O. Zinsou (SBN: 295458)
9 zinsou@braunhagey.com

10 351 California Street, Tenth Floor
11 San Francisco, CA 94104
12 Tel & Fax: (415) 599-0210

JUST FUTURES LAW

Sejal R. Zota (admitted *pro hac vice*)
sejal@justfutureslaw.org
Dinesh McCoy (admitted *pro hac vice*)
dinesh@justfutureslaw.org

95 Washington Street, Suite 104-149
Canton, MA 02021
Tel: (919) 698-5015

Attorneys for PLAINTIFFS VALERIA
THAIS SUÁREZ ROJAS, REYNA
MALDONADO, LISA KNOX, MALKIA
DEVICH CYRIL, MIJENTE SUPPORT
COMMITTEE, and NORCAL RESIST
FUND

10 **SUPERIOR COURT OF THE STATE OF CALIFORNIA**
11 **COUNTY OF ALAMEDA**

13 VALERIA THAIS SUÁREZ ROJAS, REYNA
14 MALDONADO, LISA KNOX, MALKIA
15 DEVICH CYRIL, MIJENTE SUPPORT
16 COMMITTEE, and NORCAL RESIST FUND,

17 Plaintiffs,

18 v.

19 CLEARVIEW AI, INC., COUNTY OF
20 ALAMEDA, CITY OF ALAMEDA, CITY OF
21 EL SEGUNDO, CITY OF ANTIOCH, SAN
22 LUIS OBISPO COUNTY SHERIFF’S OFFICE,
23 LAKE COUNTY SHERIFF’S DEPARTMENT,
24 and DOES 1-10,

25 Defendants.

Case No.: RG21096898

FIRST AMENDED COMPLAINT

JURY TRIAL DEMANDED

1 Plaintiffs Valeria Thais Suárez Rojas, Reyna Maldonado, Lisa Knox, Malkia Devich Cyril,
2 Mijente Support Committee, and NorCal Resist Fund allege as follows:

3 **INTRODUCTION**

4 1. Plaintiffs are two community-based organizations and four political activists. They
5 bring this action under California law to enjoin Defendant Clearview AI, Inc. (“Clearview”) from
6 illegally acquiring, storing, and selling their likenesses, and the likenesses of millions of
7 Californians, in its quest to create a cyber surveillance state. Plaintiffs also seek to enjoin California
8 law enforcement agencies who aid and abet Clearview’s illegal practices. The agencies’ use of
9 Clearview’s illegal surveillance system chills the free speech and association rights of Californians.

10 2. Defendant Clearview is a company with ties to alt-right and white supremacist
11 organizations. Clearview has built the most dangerous facial recognition database in the nation by
12 illicitly collecting over three billion photographs of unsuspecting individuals. Clearview’s database
13 is almost seven times the size of the FBI’s. Clearview has provided thousands of governments,
14 government agencies, and private entities access to its database, which they can use to identify
15 people with dissident views, monitor their associations, and track their speech. As expressly
16 intended by Clearview’s creators and early investors, its mass surveillance technology
17 disproportionately harms immigrants and communities of color.

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

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

1 5. Clearview’s end product is facial recognition technology that claims to enable its
2 users to identify virtually anyone simply by uploading a photograph. Users, like Defendants
3 County of Alameda, City of Alameda, City of El Segundo, City of Antioch, San Luis Obispo
4 County Sheriff’s Office, and Lake County Sheriff’s Department (“Municipal Defendants”) can
5 photograph a stranger at a political rally or house of worship, upload the photo to Clearview’s
6 database, and instantly see other photographs of the same person linked to various social media
7 platforms and websites. The websites often describe the person’s address, employment information,
8 political affiliations, religious activities, and familial and social relationships, among other sensitive
9 information. With Clearview, users can access all this information on their phones with the tap of a
10 finger. Clearview’s portable surveillance technology thus provides instantaneous access to almost
11 every aspect of our digital lives.

12 6. Clearview has licensed its database to governments around the world, large-scale
13 retailers, and law enforcement agencies throughout the United States, including Municipal
14 Defendants. According to news reports, by February 2020, people associated with 2,228
15 companies, law enforcement agencies, and other institutions had collectively performed nearly
16 500,000 searches of Clearview’s faceprint database. In August 2020, Clearview’s CEO bragged
17 that over 2,400 police agencies were using Clearview.

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

23 8. Multiple municipalities and law enforcement agencies in the United States have also
24 banned Clearview and other facial recognition technology, in part because of the potential for
25 abuse, false positives, and image manipulation. Studies have found empirical evidence of racial,
26

27 _____
28 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>.

1 gender, and age bias in facial recognition technology—with Asian people and African Americans
2 100 times more likely to be misidentified than white men.

3 9. Nonetheless, Clearview continues to sell access to its database to California police
4 agencies and U.S. Immigration and Customs Enforcement (ICE). This is not happenstance; one
5 person who helped build Clearview stated in 2017 that the purpose of the technology was to “ID all
6 the illegal immigrants for the deportation squads.” ICE can deploy Clearview’s technology even in
7 cities and counties that have banned the use of facial recognition technology, including multiple
8 cities in Alameda County.

9 10. In particular, the City of Alameda banned the use of facial recognition technology in
10 2019. Nevertheless, a published article revealed that police officers employed by the City
11 continued to use Clearview, having run some 550 searches until at least February 2020.²
12 Employees of the Alameda County District Attorney’s office have also run searches using
13 Clearview and police and sheriff departments in the City of El Segundo, the City of Antioch, Lake
14 County, and San Luis Obispo County have Clearview subscriptions.

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

23
24
25 ² Ryan Mac, et. al., *How a Facial Recognition Took Found Its Way into Hundreds of U.S. Police*
26 *Departments, Schools, and Taxpayer-Funded Organizations*, BUZZFEED NEWS, (Apr. 6, 2021),
27 <https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition>; Ryan
28 Mac, et. al., *Your Local Police Department Might Have Used this Facial Recognition Tool to*
Surveil You. Find Out Here, BUZZFEED NEWS, (Apr. 6, 2021),
<https://www.buzzfeednews.com/article/ryanmac/facial-recognition-local-police-clearview-ai-table>.

PARTIES

I. PLAINTIFFS

12. Plaintiff Valeria Thais Suárez Rojas (“Plaintiff Suárez”) is a resident of Alameda County and formerly worked as the Youth Organizer at California Immigrant Youth Justice Alliance (CIYJA), where they were a vocal advocate on behalf of immigrant rights. They continue to work on immigrant rights issues in the Bay Area. Plaintiff Suárez is an immigrant themselves, and has engaged in political speech critical of the police, ICE, immigration policy, and government entities. Plaintiff Suárez has uploaded photos of themselves on several social media platforms including Twitter, Instagram, Facebook, and Venmo. They have included pictures of themselves with their friends and family on these platforms, and their friends and family have also posted pictures including Plaintiff Suárez. They frequently use their social media accounts as activism tools, and post content related to their political views on these platforms. Specifically, Plaintiff Suárez has used their 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 their social media accounts private in early 2020. While they occasionally make their accounts public to support fundraising campaigns, the accounts usually remain private. However, others have continued to post photos of Plaintiff Suárez on social media platforms. On information and belief, Clearview has captured their biometric data and stored it in its faceprint database, including images of their face that are no longer publicly accessible. Plaintiff Suárez has never consented to Clearview collecting or using their image or their 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

1 media platforms including Twitter, Instagram, Facebook, and Venmo, and she has uploaded photos
2 of herself, including photographs of herself with friends and family, on these platforms. Plaintiff
3 Knox frequently uses her social media accounts as activism tools and has posted content critical of
4 police and ICE. On information and belief, Clearview has captured her biometric data and stored it
5 in its faceprint database. Plaintiff Knox has never consented to Clearview collecting or using her
6 image or biometric data.

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

21 15. Plaintiff Malkia Devich Cyril (“Plaintiff Cyril”) is a resident of Alameda County
22 and the Senior Fellow and Founding Director of MediaJustice, a grassroots organization fighting
23 for racial, economic, and gender justice in a digital age. MediaJustice has recently focused on
24 challenging the use of invasive technology in the context of policing and the criminal legal system,
25 as well as ensuring that people of color have the communications tools to amplify their voices
26 effectively. Plaintiff Cyril has worked with MediaJustice since it was founded in 2009 and has
27 championed the media and technology rights of communities of color and other under-represented
28 groups to demand and win equity in a digital age. Plaintiff Cyril frequently uses social media for

1 both personal and professional purposes and has public-facing Facebook and Twitter accounts, as
2 well as private Instagram and a personal Facebook account, where they express their views on
3 political topics and policy advocacy. Plaintiff Cyril has been a public advocate on issues of police
4 violence and abuse in both their personal and professional capacities, and they have participated in
5 numerous protests including during the George Floyd uprisings and many protests against anti-
6 Black violence between 2014-2016. On information and belief, Clearview has captured Plaintiff
7 Cyril's biometric data and stored it in its faceprint database. Plaintiff Cyril has never consented to
8 having Clearview collect or use their image or biometric data.

9 16. Plaintiff NorCal Resist, a California corporation, is a grassroots, membership-based
10 organization working to equip impacted communities with the tools needed to fight immigration
11 injustice. Plaintiff NorCal Resist has a significant interest in ensuring that immigrant and activists'
12 rights are respected and upheld, including their rights to safety and privacy. Plaintiff NorCal Resist
13 hosts Know Your Rights trainings relating to direct actions and navigating encounters with ICE and
14 police, assists with rapid response to support local residents targeted in immigration enforcement
15 actions, and has a bail fund that supports community members arrested in racial justice protests or
16 for immigration-related charges. Plaintiff NorCal Resist has close to 7,000 members throughout
17 Northern California, including more than 200 members in Alameda County. Members support the
18 organization by donating money and volunteering to support local actions and events, and members
19 vote on the leadership of the organization. NorCal Resist members have been critical of ICE,
20 immigration policy, and policing tactics, and they have expressed concern through both their
21 conduct and speech in relation to their work with Plaintiff NorCal Resist. On information and
22 belief, the biometric information and identifiers of many members of Plaintiff NorCal Resist have
23 been, and will continue to be, captured in Clearview's database without their consent. Clearview's
24 practices pose a threat to Plaintiff NorCal Resist's members by divesting them of the power to
25 control their biometric identifiers, and by chilling their ability to exercise various constitutional
26 rights—including the right to protest and to travel—without being instantaneously identified and
27 tracked.

28

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

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

1 **II. DEFENDANTS**

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



12 20. Clearview founder Hoan Ton-That, as well as several people associated with
13 Clearview, have a history of longstanding ties to the alt-right, a far-right ideology based on the
14 belief that white identity is under attack. Persons with ties to Clearview include “pizzagate”
15 conspiracy theorist Mike Cernovich; neo-Nazi hacker and *The Daily Stormer* webmaster, Andrew
16 Auernheimer; former chief technology officer of Business Insider who marched with neo-Nazis in
17 Charlottesville, Virginia, Pax Dickinson; and former Breitbart writer, Charles Johnson. In a
18 Facebook post, Johnson described “building algorithms to ID all the illegal immigrants for the
19 deportation squad,” likely referring to Smartcheckr, Defendant’s name before being rebranded to
20 “Clearview.” Marko Jukic is a former Clearview employee whose job included pitching Clearview
21 to law enforcement agencies. In 2015, he wrote that he “wholeheartedly endorse[s] racism,
22 racialism, ethnocentrism, Islamophobia, Eurocentrism and anti-Semitism.” Writing under a
23 pseudonym, Jukic described diversity and equality as “indisputably corrosive to civilization,” and
24 said that “violence most definitely is the answer.”

25 21. Clearview has registered as a data broker in the State of California. It has sold
26 licenses to policing agencies such as the City of El Segundo’s Police Department. It promotes and
27 markets its faceprint database throughout the State of California, in part by offering trial use. The
28 Los Angeles Police Department, Long Beach Police Department, San Diego Police Department,

1 San Diego District Attorney’s Office, Orange County Sheriff’s Office, and San Mateo Sheriff’s
2 Office, as well as multiple other state and local agencies, have all used Clearview on a trial basis.
3 Additionally, Clearview engages in the widespread collection of California residents’ images and
4 biometric information without notice or consent. On information and belief, Clearview illicitly
5 scrapes images of thousands of people from websites and platforms owned and operated by
6 California-based companies, such as Facebook.

7 22. Defendant County of Alameda is a county in California.

8 23. Defendant City of Alameda is a city within Alameda County, California.

9 24. Defendant City of Antioch is a city within Contra Costa County, California.

10 25. Defendant City of El Segundo is a city within Los Angeles County, California.

11 26. Defendant San Luis Obispo County Sheriff’s Office is a sheriff department in San
12 Luis Obispo County, California.

13 27. Defendant Lake County Sheriff’s Department is a sheriff department in Lake
14 County, California.

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

17 **JURISDICTION AND VENUE**

18 29. The Court has personal jurisdiction over Clearview pursuant to California Code of
19 Civil Procedure § 410.10 because Clearview conducts business transactions in California; has
20 intentionally availed itself of the laws and markets of California through the use, promotion, sale,
21 marketing, and/or distribution of its products and services at issue in this Complaint; unlawfully
22 acquires and profits from the biometric data of California residents; has committed unlawful acts
23 arising from and related to its conduct and activity in California complained of in this complaint;
24 and has committed unlawful acts expressly aimed at California residents from which this action
25 arises. The Court has personal jurisdiction over County of Alameda, City of Alameda, City of El
26 Segundo, City of Antioch, San Luis Obispo County Sheriff’s Office, and Lake County Sheriff’s
27 Department pursuant to Code of Civil Procedure § 410.10 because they are located within the State
28 of California.

1 their terms of service with their respective users. Therefore, even if a user consents to a website's
2 terms of service, that consent does not extend to Clearview's scraping.

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

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

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

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

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

27 40. Clearview maintains a log of all searches ever conducted in its database by anyone.
28 Clearview also appears to monitor searches clients run on its database. After a reporter asked police

1 officers to upload a probe image of her into Clearview’s database, for example, the company told
2 the officers that they should not be speaking to the media.

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

11 42. Facial recognition algorithms have repeatedly been shown to perform poorly when
12 examining the faces of people of color. Consequently, facial recognition technology has a far
13 greater risk of misidentifying people of color. Multiple municipalities, including San Francisco and
14 Oakland, have rejected facial recognition technology for that very reason. For example, a recent
15 study by the National Institute of Standards and Technology (NIST) found that a majority of facial
16 surveillance software exhibits racial bias.³ According to that study, African American and Asian
17 people are up to 100 times more likely to be misidentified by a facial recognition system than white
18 men, depending on the algorithm and use case.⁴

19 **B. Who Can Access Clearview**

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

22
23 _____
24 ³ Patrick Grother, Mei Ngan, & Kayee Hanaoka, Nat’l Inst. of Standards and Tech., U.S. Dep’t of
25 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>.

26 ⁴ These “demographic differentials” in error rates are severe enough that in 2019, members of
27 Congress called on the Trump administration to reconsider its plans to expand the use of facial
28 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/>.

1 44. Of particular concern, the Clearview database allows law enforcement agencies not
2 only to identify people in public spaces, but also to learn those people’s professional roles,
3 religious affiliations, familial connections and friendships, romantic partnerships, personal
4 activities, political views, patterns of travel, and even home addresses, all without receiving
5 consent, obtaining a warrant, or providing probable cause to conduct a search.

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

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

13 47. Clearview has a history of data breaches. In February 2020, hackers gained access to
14 Clearview’s client list. Clearview responded to the breach by stating that “data breaches are part of
15 life in the 21st Century.”

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

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

26 **II. POLICE AND IMMIGRATION ENFORCEMENT AGENCIES USE CLEARVIEW**

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

1 51. Further, one of Clearview’s main marketing strategies has been to offer free trials to
2 hundreds of police agencies, leading to experimental and unauthorized use. Many leaders at these
3 agencies, when contacted by the press, claimed they were unaware that employees were using the
4 tool. Clearview has promoted free trials to several police agencies across California including
5 Orange County Sheriff’s Department, Fresno Police Department, Santa Monica Police Department,
6 Long Beach Police Department, Los Angeles Police Department, Chula Vista Police Department,
7 Emeryville Police Department, Fremont Police Department, Napa Special Investigations Bureau,
8 Santa Ana Police Department, and San Diego Police Department—and several of these agencies
9 have accepted its offer.

10 52. Clearview’s marketing materials tout “unlimited searches” and encourage officers
11 not to “stop at one search.” They also suggest that officers “search a celebrity to see how powerful
12 the technology can be.”

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

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

23 55. On August 12, 2020, Clearview entered into a purchase order contract in which ICE
24 agreed to pay \$224,000 for “clearview licenses.”

25 56. Plaintiffs’ concerns about being targeted and misidentified are not abstract—ICE
26 has a history of collection of biometric data to use against vulnerable populations. Since 2015, for
27 example, ICE has performed thousands of faceprint searches on state DMV databases,
28 unbeknownst to license holders, to identify, locate, and deport individuals. ICE has conducted these

1 searches in at least three states that allow undocumented immigrants to obtain a license or driver
2 privilege card. ICE runs these searches without a warrant or any other official approval.

3 57. Plaintiffs' concerns are heightened in light of ICE's history, including its recent role
4 in family separation, its longstanding practice of detaining people in horrific conditions, and its
5 pattern of racial and religious profiling. ICE has also systematically surveilled, detained, and
6 deported immigrant activists who speak out about immigration policies and practices. For example,
7 ICE has targeted Maru Mora-Villalpando, a member of both La Resistencia and Mijente, because
8 of her "anti-ICE protests." Ravi Ragbir was arrested, at his ICE check-in meeting, after protests
9 that ICE characterized as an unwanted "display of wailing kids and wailing clergy." Daniela
10 Vargas was arrested as she left a press conference supporting the DACA program. A number of
11 immigrant rights groups and immigrants have sued ICE for violating their rights to speak,
12 assemble, and associate under the First Amendment.

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

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

1 60. Senator Markey also wrote to former Attorney General William Barr, expressing
2 concern about the DOJ’s surveillance of Black Lives Matter protesters and potential use of
3 Clearview as part of that surveillance.⁵

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

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

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

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

21 **III. DEFENDANTS VIOLATE PLAINTIFFS’ RIGHTS**

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

27 _____
28 ⁵ 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>.

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

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

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

21 69. Similarly, Confidential Member 2 is a resident of Alameda County and an active
22 member of Mijente. Confidential Member 2 regularly criticizes ICE and police practices, and
23 engages in numerous organizing efforts around the Bay Area to promote immigrant rights.
24 Confidential Member 2 is active on Facebook and Twitter, and frequently posts content critical of
25 immigration enforcement policies. His Facebook account is private, and he removed his name and
26 face image from Twitter in early 2021 because of concerns about his privacy and potential use of
27 his images without his consent. On information and belief, Clearview has captured his images,
28 extracted his biometric information, and converted them into faceprints for Clearview's faceprint

1 database. Confidential Member 2 has never given Clearview consent to do so. Learning that he is in
2 the database where he can be identified has caused him to suffer mental anguish.

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

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

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

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

24 74. Each day that Clearview is allowed to continue its illegal activities, Plaintiffs suffer
25 immediate and irreparable injuries, including chilling of their core constitutional rights of freedom
26 of association and freedom of speech, injuries to their rights to privacy, injuries to their property
27 rights in their own likenesses and biometric information, and injuries to their peace of mind and
28 wellbeing.

1 name or likeness to defendant’s advantage, commercially or otherwise; (3) lack of consent; and
2 (4) resulting injury.” *Eastwood v. Superior Court*, 149 Cal. App. 3d 409, 417 (1983).

3 80. Without providing notice to or obtaining consent from Plaintiffs and Plaintiffs’
4 members, Clearview knowingly and surreptitiously collected Plaintiffs’ and Plaintiffs’ members’
5 names, photographs, biometric information, and other identifiers (which constitute Plaintiffs’ and
6 Plaintiffs’ members’ “identities”) by scraping images from websites in violation of many of the
7 websites’ policies prohibiting such conduct.

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

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

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

25 **SECOND CAUSE OF ACTION**

26 **Invasion of Privacy Under California Constitution art. 1, § 1**
27 **(Against Defendants Clearview and Does 1-10)**

28 84. Plaintiffs incorporate all preceding paragraphs as though set forth herein.

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

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

11 87. Plaintiffs and Plaintiffs’ members also have legally protected interests in their
12 associational privacy, which is a component of both informational and autonomy privacy.

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

19 89. Clearview’s invasion of Plaintiffs’ and Plaintiffs’ members’ privacy is serious and
20 highly offensive for three reasons: first, because Clearview’s conduct is surreptitious, in violation
21 of websites’ terms of service, and in violation of numerous cease-and-desist letters from such
22 websites; second, because Clearview extracts biometric information from Plaintiffs’ immutable
23 physical characteristics, such that once Clearview enters an individual into its database, that
24 individual permanently loses anonymity and privacy; and third, because it places Plaintiffs’ and
25 Plaintiffs’ members lives and livelihood in danger, both from being misidentified to law-
26 enforcement and immigration agencies and from being correctly identified and targeted for
27 retaliation for their public political stances.

28

1 **THIRD CAUSE OF ACTION**

2 **Business & Professions Code §§ 17200, et seq.**
3 (Against Defendants Clearview and Does 1-10)

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

5 91. The Unfair Competition Law (“UCL”) prohibits, *inter alia*, any unlawful or unfair
6 business practice. Clearview’s conduct is both unlawful and unfair because it violates CAL. CONST.
7 art. 1, § 1, CAL. PENAL CODE § 502, California’s common-law right against appropriation of
8 likeness, and the terms of use of the various websites where Clearview scraped the data.

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

19 **FOURTH CAUSE OF ACTION**

20 **Aiding and Abetting the Torts of Common Law Appropriation of Likeness
21 & Invasion of Privacy Under California Constitution art. 1, § 1**
22 (Against Municipal Defendants and Does 1-10)

23 93. Plaintiffs incorporate all preceding paragraphs as though set forth herein.

24 94. Liability may be imposed on one who aids and abets the commission of an
25 intentional tort if the person (a) knows the other’s conduct constitutes a breach of duty and gives
26 substantial assistance or encouragement to the other to so act or (b) gives substantial assistance to
27 the other in accomplishing a tortious result and the person’s own conduct, separately considered,
28 constitutes a breach of duty to the third person.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28


PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully pray for the following:

- A. Injunctive relief;
- B. Compensatory damages;
- C. An award of attorney’s fees and costs; and
- D. Any other relief as equity and justice may require.

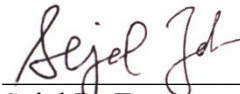
Dated: December 16, 2022

Respectfully submitted,
BRAUNHAGEY & BORDEN LLP



Ellen V. Leonida

JUST FUTURES LAW



Sejal R. Zota

Attorneys for Plaintiffs Valeria Thais Suárez
Rojas, Reyna Maldonado, Lisa Knox, Malkia
Devich Cyril, Mijente Support Committee, and
Norcal Resist Fund

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

DEMAND FOR JURY TRIAL

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

Dated: December 16, 2022

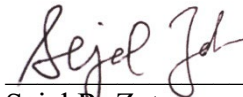
Respectfully submitted,

BRAUNHAGEY & BORDEN LLP



Ellen V. Leonida

JUST FUTURES LAW



Sejal R. Zota

Attorneys for Plaintiffs Valeria Thais Suárez Rojas, Reyna Maldonado, Lisa Knox, Malkia Devich Cyril, Mijente Support Committee, and Norcal Resist Fund