From: Samuel Ridge	Fax: 14155990210	То:	Fax: (510) 267-1546	Page: 4 of 30	04/21/2021 2:58 PM
3 4 5 6 7 8 9 10 11 12 13 14	leonida@braunh Matthew Borden, J borden@braunha J. Noah Hagey, Es hagey@braunha Athul K. Acharya, acharya@braunh Gunnar K. Martz, martz@braunhag BRAUNHAGEY 351 California Stre San Francisco, CA Telephone: (415) 5 Sejal R. Zota (pro sejal@justfuture Dinesh McCoy (pri dinesh@justfuture JUST FUTURES I 95 Washington Str Canton, MA 0202 Telephone: (919) 6 Attorneys for PLA RENDEROS, VAI ROJAS, REYNA J KNOX, MIJENTE	Esq. (SBN: 214323) agey.com q. (SBN: 262331) gey.com Esq. (SBN: 315923) agey.com Esq. (SBN: 315923) agey.com Esq. (SBN: 300852) gev.com & BORDEN LLP eet, Tenth Floor , 94104 599-0210 pac vice application for slaw.org p hac vice application for eslaw.org p hac vice application for eslaw.org LAW reet, Suite 104-149 1 598-5015 INTIFFS STEVEN LERIA THAIS SUÁRI MALDONADO, LISA	forthcoming) forthcoming) EZ	FILED BY FA ALAMEDA COUNT April 22, 2021 CLERK OF THE SUPERIOR COO By Milagros Cortez, D CASE NUMBER: RG210968	Y JRT Deputy
18					
19		COUNTY OF ALAMEDA			
20 21 22 23 24 25 26 27 28	SUÁREZ ROJAS, LISA KNOX, MIJ COMMITTEE, an V. CLEARVIEW AI, DISTRICT ATTO DEPARTMENT, J DEPARTMENT, J DEPARTMENT, 3	d NORCAL RESIST F intiffs, INC., ALAMEDA CO RNEY, ALAMEDA P EL SEGUNDO POLIC ANTIOCH POLICE	DO, UND, OUNTY OLICE	INT IAL DEMANDE	 D
	COMPLAINT				

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

3

# **INTRODUCTION**

- 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. Plaintiffs also seek to enjoin California
   law enforcement agencies who aid and abet Clearview's illegal practices. The agencies' use of
   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 organizations. Clearview has built the most dangerous facial recognition database in the nation by 11 illicitly collecting over three billion photographs of unsuspecting individuals. Clearview's database 12 is almost seven times the size of the FBI's. Clearview has provided thousands of governments, 13 government agencies, and private entities access to its database, which they can use to identify 14 15 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 16 17 disproportionately harms immigrants and communities of color.
- 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 1 2 users to identify virtually anyone simply by uploading a photograph. Users, like Defendant law 3 enforcement agencies, 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 4 5 various social media platforms and websites. The websites often describe the person's address, employment information, political affiliations, religious activities, and familial and social 6 7 relationships, among other sensitive information. With Clearview, users can access all this 8 information on their phones with the tap of a finger. Clearview's portable surveillance technology 9 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, including Defendant law
 enforcement agencies. 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.

16 7. Clearview has been banned internationally. Canada has asked Clearview to remove
17 the faces of Canadian residents from its database, because "what Clearview does is mass
18 surveillance"—putting all Canadians "continually in a police lineup."<sup>1</sup> Similarly, the European
19 Union recently found, after an 11-month investigation, that Clearview's practices violate its
20 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 Asian people and African Americans
 100 times more likely to be misidentified than white men.

- 26
- 27

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

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

10. In particular, the City of Alameda banned the use of facial recognition technology in
2019. Nevertheless, a recently published article revealed that police officers employed by the City
continue to use Clearview, having run some 550 searches until at least February 2020. Employees
of the Alameda County District Attorney's office have also run searches using Clearview. And
police departments in the City of El Segundo and the City of Antioch have active Clearview
subscriptions.<sup>2</sup>

13 11. 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 14 15 capacities. Plaintiffs Mijente Support Committee ("Mijente") and NorCal Resist Fund ("NorCal Resist") are two immigrant rights, membership-based organizations representing the interests of 16 thousands of California residents. The ability to control their likenesses and biometric identifiers-17 18 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 19 20 their missions. 21 22 23 24 25 <sup>2</sup> Ryan Mac, et. al., How a Facial Recognition Took Found Its Way into Hundreds of U.S. Police Departments, Schools, and Taxpayer-Funded Organizations, BUZZFEED NEWS, (Apr. 6, 2021), 26 https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition; Ryan Mac, et. al., Your Local Police Department Might Have Used this Facial Recognition Tool to 27 Surveil You. Find Out Here, BUZZFEED NEWS, (Apr. 6, 2021), 28 https://www.buzzfeednews.com/article/ryanmac/facial-recognition-local-police-clearview-ai-table. 3

1 2

#### **PARTIES**

### A. Plaintiffs

3 12. 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 4 5 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 6 7 legal system, as well as ensuring that people of color have the communications tools to amplify 8 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. 9 10 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 11 purposes of political and policy advocacy. Plaintiff Renderos is frequently critical of police and 12 13 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 14 15 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 16 biometric data. 17

13. 18 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 19 20Alliance (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 themself, and 21 has engaged in political speech critical of the police, ICE, immigration policy, and government 22 entities. Plaintiff Suárez has uploaded photos of themself on several social media platforms 23 24 including Twitter, Instagram, Facebook, and Venmo. They have included pictures of themself with 25 their friends and family on these platforms, and their friends and family have also posted pictures 26 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 27 used their social media accounts to criticize ICE and raise money for community members recently 28

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.

8 14. 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 9 10 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 11 Centro Legal de la Raza, where she helped found and manage the detained representation project. 12 Plaintiff Knox oversaw emergency legal services for Alameda County's rapid response network 13 and managed legal clinics at two California detention centers. Plaintiff Knox participates in and 14 15 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 16 of herself, including photographs of herself with friends and family, on these platforms. Plaintiff 17 18 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 19 20in its faceprint database. Plaintiff Knox has never consented to Clearview collecting or using her image or biometric data. 21

15. 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.

8 16. Plaintiff NorCal Resist, a California corporation, is a grassroots, membership-based organization working to equip impacted communities with the tools needed to fight immigration 9 10 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 11 hosts Know Your Rights trainings relating to direct actions and navigating encounters with ICE and 12 police, assists with rapid response to support local residents targeted in immigration enforcement 13 actions, and has a bail fund that supports community members arrested in racial justice protests or 14 15 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 16 17 organization by donating money and volunteering to support local actions and events, and members 18 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 19 20conduct 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 21 been, and will continue to be, captured in Clearview's database without their consent. Clearview's 22 practices pose a threat to Plaintiff NorCal Resist's members by divesting them of the power to 23 24 control their biometric identifiers, and by chilling their ability to exercise various constitutional 25 rights—including the right to protest and to travel—without being instantaneously identified and tracked. 26

27 17. Plaintiff Mijente, an Arizona corporation, is a national digital and grassroots hub for
28 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 1 2 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 3 increasing technological capabilities of corporations and the government, and has a significant 4 5 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 6 7 whom have, at times, uploaded their photos to various internet-based platforms and websites, and 8 have engaged in political speech that could be considered critical of the police, ICE, immigration 9 policy, and government entities. Plaintiff Mijente's members have specifically criticized law 10 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 11 and identifiers have been, and will continue to be, captured in Clearview's database without their 12 consent. Clearview's practices pose a threat to Plaintiff Mijente's members by divesting them of 13 the power to control their biometric identifiers, and by chilling their ability to exercise various 14 15 constitutional rights-including the right to protest and to travel-without being instantaneously identified and tracked. 16

18. Plaintiffs Suárez, Knox, Maldonado, and Renderos, as well as members of Plaintiffs 17 NorCal Resist and Mijente, did not consent to have their biometric data harvested by Clearview, 18 did not understand that their biometric data could or would be obtained by Clearview or anyone 19 20else 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: 21 expenditure of resources in understanding the extent of Clearview's misappropriation of their and 22 their members' identities, images, likenesses, and biometric data; loss of their property rights in 23 24 their own identities, images, likenesses, and biometric data; mental anguish as a result of the 25 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. 26

- 27
- 28

## B. Defendants

1

2

3

4

5

6

7

8

9

19. 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, above) and Richard
 Schwartz, a former aide to Rudy Giuliani, Esq.

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

21. 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 1 2 Sheriff's Office, as well as multiple other state and local agencies, have all used Clearview on a trial basis. Additionally, Clearview engages in the widespread collection of California residents' 3 images and biometric information without notice or consent. On information and belief, Clearview 4 5 illicitly scrapes images of thousands of people from websites and platforms owned and operated by California-based companies, such as Facebook. 6 22. 7 Defendant Alameda County District Attorney is a department of Alameda County in 8 California.

9 23. Defendant Alameda Police Department is a police department in the city of
10 Alameda, within Alameda County.

11 24. Defendant Antioch Police Department is a police department in the city of Antioch,
12 within Contra Costa County.

13 25. Defendant El Segundo Police Department is a police department in the city of El
14 Segundo, within Los Angeles County.

15 26. 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

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

28

28. Venue is proper in Alameda County pursuant to California Code of Civil Procedure
 §§ 394, 395.5 because Plaintiffs' injuries occurred in Alameda County; 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; Defendants Alameda
 County District Attorney and Alameda Police Department are located within Alameda County; and
 this Court is located within Alameda County.

7

8

#### FACTUAL ALLEGATIONS

## I. DEFENDANT CLEARVIEW'S FACIAL RECOGNITION TECHNOLOGY

9

#### A. How Clearview Constructs Its Illegal Database

29. 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.

30. 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.

31. 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.

32. Multiple online entities, including Google, YouTube, Facebook, Venmo, LinkedIn,
and Twitter, have requested that Clearview cease and desist from 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.

3 33. 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.

9 34. 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 35. During the recognition step, Clearview uses its facial recognition AI to search,
15 identify, classify, and index faceprints in its database.

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

37. 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."

27 38. 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

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.

~

3 39. Because Clearview extracts biometric information from images, its database contains physical characteristics of individuals. Individuals can change their characteristics only 4 through extreme means like plastic surgery. Therefore, once Clearview enters an individual into its 5 database, that individual permanently loses anonymity and privacy. Indeed, Clearview allows 6 anyone with access to its database to capture a single photo of an individual, and with a few 7 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.

40. 11 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 12 13 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 14 15 study by the National Institute of Standards and Technology (NIST) found that a majority of facial surveillance software exhibits racial bias.<sup>3</sup> According to that study, African American and Asian 16 people are up to 100 times more likely to be misidentified by a facial recognition system than white 17 men, depending on the algorithm and use case.<sup>4</sup> Clearview has refused to participate in NIST's 18 Facial Recognition Vendor Test Program or any other meaningful, independent review. 19

20

# B. Who Can Access Clearview

21

41. By February 2020, Clearview had shared its technology with more than 2,200 law

- 22
- <sup>3</sup> 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), <u>https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf</u>.

enforcement departments, government agencies, and private companies across 27 countries.

- <sup>4</sup> 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),

<sup>28 &</sup>lt;u>https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/</u>.

42. 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,
 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.

6 43. 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 44. 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 45. 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 46. 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 the19 lobby of a residential building.

47. 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
   48. According to Clearview, over 2,400 law enforcement agencies at both the federal
   and the state level have used its technology since January 2019.
  - 13

49. Further, one of Clearview's main marketing strategies has been to offer free trials to 1 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, Santa Ana Police Department, and San Diego Police Department-and several of these agencies 8 have accepted its offer. 9

10 50. 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 51. 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 52. 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 53. On August 12, 2020, Clearview entered into a purchase order contract in which ICE
24 agreed to pay \$224,000 for "clearview licenses."

54. 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,

28 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.

2

55. Plaintiffs' concerns are heightened in light of ICE's history, including its recent role 3 in family separation, its longstanding practice of detaining people in horrific conditions, and its 4 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 immigrant rights groups and immigrants have sued ICE for violating their rights to speak, 11 assemble, and associate under the First Amendment. 12

13 56. Federal agencies, including DHS and its subsidiaries, also have a history of conducting intrusive surveillance on protestors associated with the Black Lives Matter movement. 14 15 A leaked memorandum shows that the Department of Justice ("DOJ") authorized the Drug Enforcement Administration to "conduct covert surveillance" and collect intelligence on people 16 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 States. CBP agents detained protestors, abducting them from the streets of Portland despite a lack 19 20 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 21 situational awareness at the request of our federal law enforcement partners in Minneapolis." 22

57. 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."

58. 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.<sup>5</sup>

4 59. 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 60. 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 61. 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 62. 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 VIOLATES PLAINTIFFS' RIGHTS**

63. 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

27

<sup>28 &</sup>lt;sup>5</sup> Letter from Senator Edward J. Markey to Attorney General William Barr (June 11, 2020), <u>https://www.markey.senate.gov/imo/media/doc/DOJ%20Protest%20Surveillance.pdf</u>.

violation of the laws identified in this Complaint, and without notice to, or permission from,
 Plaintiffs.

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

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

13 66. 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 14 15 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 16 Facebook, where he has a private account (but a publicly accessible profile page on which his 17 18 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 19 20biometric 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 21 database where he can be identified has caused him to suffer mental anguish. 22

67. 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.

68. 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.

69. 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.

70. Plaintiffs Suárez, Knox, Maldonado, and Renderos, as well as members of Plaintiffs 13 NorCal Resist and Mijente, have suffered multiple injuries as a result of Clearview's actions, 14 15 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 16 suffered loss and diminution of their property rights in their own identities, images, likenesses, and 17 18 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 19 20immigration status and misidentified by Clearview's system.

71. 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.

26 72. Each day that Clearview is allowed to continue its illegal activities, Plaintiffs suffer
27 immediate and irreparable injuries, including chilling of their core constitutional rights of freedom
28 of association and freedom of 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.

73. The City of Alameda banned the use of facial recognition in December 2019. Prior 3 to that ban, Clearview's co-founder corresponded with the Alameda Police Department about 4 convincing the City of Alameda to pay for a Clearview license. And an April, 2021 article revealed 5 that even *after* the City of Alameda banned the use of facial recognition, individuals employed by 6 the City of Alameda and Alameda County-police officers and employees of the District 7 8 Attorney's office—continued to use Clearview. They uploaded probe images to Clearview so that 9 Clearview's facial recognition software could analyze them for biometric information and search 10 for other photos with matching biometric information. Clearview also added these uploaded probe images and corresponding biometric information to its database for future searches.<sup>6</sup> 11 74. Police officers employed by the City of El Segundo and the City of Antioch have 12 also used and continue to use Clearview in the same manner: They upload probe images to 13 Clearview so that Clearview can analyze them for biometric information and search for other 14 15 photos with matching biometric information. Clearview also adds these uploaded probe images and corresponding biometric information to its database for future searches. 16 75. The use of Clearview by these municipalities chills Plaintiffs from engaging in 17 protected speech critical of the police. Plaintiffs fear being identified and targeted for retaliation by 18 members of law enforcement if they criticize law enforcement. 19 20 FIRST CAUSE OF ACTION **Common Law Appropriation of Likeness** 21 76. Plaintiffs incorporate all preceding paragraphs as though set forth herein. 22 77. Under California common law, the right against appropriation of likeness has four 23 elements: "(1) the defendant's use of the plaintiff's identity; (2) the appropriation of plaintiff's 24 25 <sup>6</sup> Ryan Mac, et. al., How a Facial Recognition Took Found Its Way into Hundreds of U.S. Police Departments, Schools, and Taxpayer-Funded Organizations, BUZZFEED NEWS, (Apr. 6, 2021), 26 https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition; Ryan Mac, et. al., Your Local Police Department Might Have Used this Facial Recognition Tool to 27 Surveil You. Find Out Here, BUZZFEED NEWS, (Apr. 6, 2021), 28 https://www.buzzfeednews.com/article/ryanmac/facial-recognition-local-police-clearview-ai-table 19 COMPLAINT

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).

3

78. 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.

8 79. 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.

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

81. Clearview'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
Clearview's advantage.

- 25
- 26
- 27

82.

28

**SECOND CAUSE OF ACTION** 

California Constitution art. 1, § 1

Plaintiffs incorporate all preceding paragraphs as though set forth herein.

83. 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.

84. 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.

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

86. 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.

87. 19 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 20of websites' terms of service, and in violation of numerous cease-and-desist letters from such 21 websites; second, because Clearview extracts biometric information from Plaintiffs' immutable 22 physical characteristics, such that once Clearview enters an individual into its database, that 23 individual permanently loses anonymity and privacy; and third, because it places Plaintiffs' and 24 25 Plaintiffs' members lives and livelihood in danger, both from being misidentified to lawenforcement and immigration agencies and from being correctly identified and targeted for 26 retaliation for their public political stances. 27

28

1	THIRD CAUSE OF ACTION								
2	Business & Professions Code §§ 17200, et seq.								
-3	88. Individual Plaintiffs incorporate all preceding paragraphs as though set forth herein.								
4	89. The Unfair Competition Law ("UCL") prohibits, <i>inter alia</i> , any unlawful or unfair								
т 5	business practice. Clearview's conduct is both unlawful and unfair because it violates California								
6	Constitution art. 1, § 1, California Penal Code § 502, California's common-law right against								
7	appropriation of likeness, and the terms of use of the various websites where Clearview scraped the								
	data.								
8 9	90. 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,								
10	biometric information and likeness, both by statute, Civ. Code §§ 3344, 3344.1, and through its								
11	common law appropriation-of-likeness tort. Clearview's use of Individual Plaintiffs' likenesses is a								
12	primary factor in private and government entities' purchases of Clearview's services. Without the								
13	likenesses of Individual Plaintiffs and others, Clearview would have no service to sell. By								
14	appropriating Individual Plaintiffs' likenesses without consent, Clearview has deprived them of the								
15	opportunity to profit by licensing such use. Additionally, individual Plaintiffs have expended								
16	resources in understanding the extent of Clearview's misappropriation of their identities, images,								
17	likenesses, and biometric data.								
18									
19	FOURTH CAUSE OF ACTION Aiding and Abetting a Tort								
20	91. Plaintiffs incorporate all preceding paragraphs as though set forth herein.								
21	92. Liability may be imposed on one who aids and abets the commission of an								
22	intentional tort if the person (a) knows the other's conduct constitutes a breach of duty and gives								
23	substantial assistance or encouragement to the other to so act or (b) gives substantial assistance to								
24									
25	the other in accomplishing a tortious result and the person's own conduct, separately considered,								
26	constitutes a breach of duty to the third person.								
27	93. Defendants Alameda County District Attorney, Alameda Police Department, El								
28	Segundo Police Department, and Antioch Police Department (Municipal Defendants) knew that								

1	Clearview's conduct described above constituted a breach of duty to Plaintiffs. That is why the City					
2	of Alameda banned the use of facial recognition technology in 2019.					
3	94. Municipal Defendants provided substantial assistance to Clearview in its tortious					
4	conduct by uploading probe photographs containing biometric information that Clearview could					
5	assimilate into its database.					
6	95. Municipal Defendants also gave encouragement to Clearview in its tortious conduct					
7	by subscribing to Clearview, paying for Clearview, and/or promoting the use of Clearview by their					
8	employees.					
9	FIFTH CAUSE OF ACTION					
10	Infringement on Plaintiffs' Liberty of Speech					
11	96. Article I, § 2(a) of the California Constitution provides: "Every person may freely					
12	speak, write and publish his or her sentiments on all subjects, being responsible for the abuse of					
13	this right. A law may not restrain or abridge liberty of speech or press."					
14	97. Municipal Defendants' use of Clearview chills Plaintiffs and Plaintiffs' members					
15	from exercising the liberty of speech granted by the California Constitution and has a chilling					
16	effect on Plaintiffs' and Plaintiffs' members' rights of association. Plaintiffs fear being identified					
17	and targeted for retribution by members of law enforcement if they criticize law enforcement.					
18	Knowing that their biometric information can be accessed by local law enforcement makes them					
19	reluctant to speak at a rally or attend a protest.					
20	98. Municipal Defendants' use of Clearview thus violates the California Constitution's					
21	guarantee of liberty of speech.					
	PRAYER FOR RELIEF					
22 23	WHEREFORE, Plaintiffs respectfully pray for the following:					
23	A. Injunctive relief;					
25	B. Compensatory damages;					
26	C. An award of attorney's fees and costs; and					
27	D. Any other relief as equity and justice may require.					
28						
_0						
	23					

1	Dated: April 21, 2021	Respectfully submitted,
2		BRAUNHAGEY & BORDEN LLP
3		
4		
5		Ellen V. Leonida
6		
7		JUST FUTURES LAW
8		Rejep lat
9		Sejal R. Zota
10		
11		Attorneys for Plaintiffs Steven Renderos, Valeria Thais Suárez Rojas, Reyna Maldonado, Lisa Knox, Mijente Support Committee, and Norcal Resist Fund
12		Lisa Knox, Mijente Support Committee, and Norcal Resist Fund
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		
		24
		COMPLAINT

1	1 DEMAND FOR	DEMAND FOR JURY TRIAL			
2	2 Plaintiffs hereby demand a jury trial of all	claims and causes of action triable before a jury.			
3	3				
4	4 Dated: April 21, 2021	Respectfully submitted,			
5	5	BRAUNHAGEY & BORDEN LLP			
6	6	126			
7	7	Ellen V. Leonida			
8	8	Ellen V. Leonida			
9	9	JUST FUTURES LAW			
10	0	JUST FUTURES LAW			
11	1	Spiel Id-			
12	2	Sejal R. Zota			
13	3				
14	4	Attorneys for Plaintiffs Steven Renderos, Valeria Thais Suárez Rojas, Reyna Maldonado, Lisa Knox, Mijente Support Committee, and Norcal Resist Fund			
15		Norcal Resist Fund			
16					
17					
18					
19					
20					
21					
22					
23					
24					
25 26					
26 27					
27					
20					
	2 COMP	5 LAINT			

I