UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

DEAN JOHN, RYAN BALFANZ, BENJAMIN JAIS, ROSEMARY ARIAS, and AIMEE ALBRECHT, on behalf of themselves and all others similarly situated,

Plaintiffs,

vs.

CLEARVIEW AI, Inc.,

Defendant.

Civil Action ________

JURY TRIAL DEMAND

CLASS ACTION COMPLAINT

Plaintiffs Dean John, Ryan Balfanz, Benjamin Jais, Rosemary Arias, and Aimee Albrecht bring this Class Action Complaint against Defendant Clearview AI, Inc., and allege as follows:

INTRODUCTION

1. Founded in 2017, Clearview AI ("Clearview") is an American, for-profit technology company that markets and licenses advanced facial recognition software that infringes the privacy and civil liberties of nearly everyone in the United States. It also violates numerous statutory and common law principles as detailed herein.

2. Since its inception, Clearview has covertly collected billions of personal photographs from across the internet, extracted biometric information from them, and aggregated that data into a massive surveillance database that can identify hundreds of millions of Americans in seconds with just a picture. Clearview created this dystopian dragnet without ever obtaining permission from the subjects of the images or the websites on which they were hosted.

3. Plaintiffs bring claims for violations of the Illinois Biometric Privacy Act, 740 ILCS 14/1, et seq.; Cal. Bus. & Prof. Code § 17200, et seq.; California Common Law Right of Publicity; California Constitutional Right to Privacy; intentional interference with contractual relations; and unjust enrichment.

CLEARVIEW'S DEVELOPMENT

4. Hoan Ton-That and Richard Schwartz Co-Founded Clearview. Mr. Ton-That has been publicly linked with extremist groups and previously ran a company that shut down after it was branded a "phishing scam."[1]

5. Police departments have had access to facial recognition tools for many years, but they have historically been limited to searching government-provided images, such as mug shots and driver's license photos. In recent years, facial recognition algorithms have improved in accuracy, but Mr. Ton-That wanted to go beyond what any previous company had accomplished and create a database of "publicly available" images from which his proprietary software could search.

6. Many of these images are posted on users' social media accounts and are not generally available to the public or in the public domain. Most major social media companies, such as Facebook, Instagram, and Twitter, prohibit precisely what Clearview was seeking to do.

7. Despite prohibitions on these activities, Clearview hired engineers to develop software that crawled the internet for images of people's faces and to create a next-generation facial recognition algorithm. The resulting system uses what Mr. Ton-That described as a "state-of-the-art neural net" to convert all the images into mathematical formulas, or vectors, based on facial geometry — like how far apart a person's eyes are.

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

8. Clearview then created a vast directory that clustered all the photos with similar vectors into “neighborhoods.” When a user uploads a photo of a face into Clearview’s system, it converts the face into a mathematical vector and then shows all the scraped photos stored in that vector’s neighborhood — along with the links to the sites from which those images came.

9. By the end of 2017, Clearview had developed a formidable facial recognition tool, which it initially called “Smartcheckr,” but Mr. Schwartz and Mr. Ton-That weren’t sure to whom they were going to sell it. “We thought of every idea,” Mr. Ton-That is reported as saying.

10. One of their initial pitches, in late 2017, was to Paul Nehlen — an anti-Semite and self-described “pro-white” politician running for Congress in Wisconsin — to use “unconventional databases” for “extreme opposition research,” according to a Smartcheckr document provided to Mr. Nehlen and later posted online.

11. The company soon changed its name to Clearview AI and began heavily marketing itself to law enforcement officials. Around this time, the company obtained its first round of funding from outside investors.

12. Clearview deployed current and former U.S. government officials to approach police forces, offering free trials and annual licenses initially for as little as $2,000. Mr. Schwartz utilized his political connections to help make government officials aware of the tool.

13. The company’s most effective sales technique was offering 30-day free trials to individual officers, who then encouraged their agency’s acquisition departments to sign up and who also praised the tool to officers from other police departments at conferences and online.

14. The company soon exploded and was openly used by thousands of law enforcement agencies throughout the country, and quietly used by private industry and the well-connected.

HOW CLEARVIEW OBTAINED ITS DATA

15. To obtain its database, Clearview "scraped" or "mined" facial pictures and data from major web platforms like Google, Facebook, YouTube, Twitter, Venmo, and millions of other websites without the consent of the people whose information was being gathered and often against the express terms of those companies who were hosting such data.[2]

16. Web "scaping" or "data mining" is a technique used to extract large amounts of data from websites using automated webcrawlers capable of efficiently extracting vast amounts of underlying information and images and saving that data in a separate database. The data "scraped" can include a full webpage or specific data selected by the scraper, such as photos and biometric data.

17. Clearview focuses on scraping user images and photographs for use in its massive database, as well as identifying information about those individuals.

18. Published reports suggest that Clearview also sought to supplement its database of web-scraped photos with mug shots, as well as photos that police departments and others upload when looking to identify targets.

19. One of the major problems with Clearview's scraping of personal data and photos is that it is done without the knowledge of the individuals whose information is being gathered or the website on which that information is hosted. Google, YouTube, Facebook, Venmo, LinkedIn, and Twitter have sent cease-and-desist letters to Clearview, as scraping or otherwise collecting user data violates those platforms' terms and conditions.[3]

[2] Ben Gilbert, *Clearview AI scraped billions of photos from social media to build a facial recognition app that can ID anyone – here's everything you need to know about the mysterious company*, https://www.businessinsider.com/what-is-clearview-ai-controversial-facial-recognition-startup-2020-3 (last accessed Mar. 10, 2020); *see also* Kashmir Hill, *supra* n.1.

[3] CBS News, *Google, YouTube, Venmo and LinkedIn send cease-and-desist letters to facial recognition app that helps law enforcement*, https://www.cbsbews.com/news/clearview-ai-google-youtube-send-cease-and-desist-letter-to-facial-recognition-app/ (last accessed Mar. 10, 2020).

20. For example, YouTube articulated that "YouTube's Terms of Service explicitly forbid collecting data that can be used to identify a person." Venmo noted that "[s]craping Venmo is a violation of our terms of service and we actively work to limit and block activity that violates these policies", while LinkedIn stated "[t]he scraping of member information is not allowed under our terms of service and we take action to protect our members."

21. Similarly, Facebook's terms of service state: "we do not allow attempts to gather sensitive user information through the abuse of our platform and products." Specifically, the terms prohibit "[a]tempt[ing] to compromise user accounts or gather sensitive information through unauthorized means," including "[g]aining access to any account or user data other than your own without explicit permission from the account owner."

22. As major tech companies have opposed Clearview's method for building an image database, Clearview has generally ignored those requests. Clearview's chief executive, Hoan Ton-That, argues that his company has a Constitutional right to aggregate and process any information it is able to access. For example, he told CBS This Morning: "There is a First Amendment right to public information. The way that we have built our system is to only take publicly available information and index it that way."[4]

23. People who post pictures of themselves on social media networks do not expect that their pictures will be copied, extracted, and made searchable, particularly where those sites prohibit these practices. Moreover, others who are tagged or identified in pictures never give consent. And Clearview scrapes and obtains pictures and data that are not generally available to the public.

[4] CEO of controversial AI startup dismisses critics (Feb. 5, 2020), https://www.youtube.com/watch?v=LpxDzV5AKfY.

HOW CLEARVIEW WORKS

24. Clearview's software identifies people using scraped images in its searchable database of over 3 *billion* photos.[5] By uploading a picture of a target about which they would like more information, a user of Clearview's software can then see photos of that person scraped from various websites, along with links to where those photos appeared and other biometric data.[6]

25. Once uploaded, Clearview's application uses its proprietary facial recognition technology to match the images uploaded to those in the database.[7]

26. The technology works differently than older facial recognition tools used by police departments, which require the subject to be looking straight ahead. Instead, Clearview's application captures images of faces taken from many different angles.

27. The Clearview platform also uses images from social media platforms even after they have been deleted by a user, and even if they are posted by someone else, without the subject's consent.

28. Contracts to use Clearview's search service can cost as much as $50,000 for a two-year license.

29. The application has been highly successful in matching uploaded images to real people. According to the *New York Times*, a detective in Clifton, N.J. urged his captain to buy

[5] Ben Gilbert, *Clearview AI scraped billions of photos from social media to build a facial recognition app that can ID anyone – here's everything you need to know about the mysterious company*, https://www.businessinsider.com/what-is-clearview-ai-controversial-facial-recognition-startup-2020-3 (last accessed Mar. 10, 2020)*; see also* Sara Morrison, *The world's scariest facial recognition company is now linked to everyone from ICE to Macy's*, https://www.vox.com/recode/2020/2/26/21154606/clearview-ai-data-breach (last accessed Mar. 10, 2020).

[6] Hill, *supra* n.1.

[7] Sara Morrison, *The world's scariest facial recognition company is now linked to everyone from ICE to Macy's*, https://www.vox.com/recode/2020/2/26/21154606/clearview-ai-data-breach (last accessed Mar. 10, 2020).

the software because it was "able to identify a suspect in a matter of seconds."[8] Clearview's CEO Hoan Ton-That has stated that the application has an accuracy rate of 99.6%.[9]

CLEARVIEW'S MARKETING

30. In an attempt to quell public outcry over its quest to create a global biometric identification system, Clearview claimed that the software is intended for use only by law enforcement agencies. "It's strictly for law enforcement," Mr. Ton-That said on Fox Business as recently as February 2020.[10]

31. Similarly, in a January 27, 2020 blog post, Clearview wrote: "Clearview AI's search engine is available only for law enforcement agencies and select security professionals to use as an investigative tool, and its results contain only public information. Accordingly, the Clearview app has built-in safeguards to ensure these trained professionals only use it for its intended purpose: to help identify the perpetrators and victims of crimes." In reality, in contrast to these public pronouncements, Clearview has marketed and sold the software much more broadly.

32. Undoubtedly, law enforcement is one of Clearview's target markets. Clearview's application has been used by more than 2,200 law enforcement departments, government agencies, and companies across 27 countries.[11] Clearview has signed paid contracts with US Immigration and Customs Enforcement and the US Attorney's Office for the Southern District of

[8] Hill, *supra* n.1.

[9] CBS News, *Google, YouTube, Venmo and LinkedIn send cease-and-desist letters to facial recognition app that helps law enforcement*, https://www.cbsbews.com/news/clearview-ai-google-youtube-send-cease-and-desist-letter-to-facial-recognition-app/ (last accessed Mar. 10, 2020).

[10] New facial recognition tech 'loved' by law enforcement: Clearview AI CEO, Fox Business (Feb. 19, 2020), https://video.foxbusiness.com/v/6133890195001/#sp=show-clips.

[11] Ryan Mac, Caroline Haskins, and Logan McDonald, *Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA*, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement (last accessed Mar. 10, 2020).

New York.[12] Clearview has credentialed users at the Federal Bureau of Investigation, Customs and Border Protection, Interpol, and hundreds of local police departments.[13]

33. In contrast to Clearview's statements, however, the company has also been aggressively pursuing clients in numerous other industries beyond governmental law enforcement, such as retail, banking, and gaming.

34. Clearview's fabrications were recently laid bare when a Clearview client list was exposed during a data breach.[14]

35. Documents from the data breach were obtained and reported on by BuzzFeed News. [15] They indicate that Clearview's facial recognition software had been provided to and used by a broad array of non-law enforcement and commercial enterprises, such as:

- Retail (Best, Buy, Kohl's, and Macy's);
- Entertainment (Madison Square Garden and Eventbrite);
- Sports (the National Basketball Association);
- Gaming and hospitality (Las Vegas Sands and Pechanga Resort);
- Fitness (Equinox);
- Finance (Coinbase cryptocurrency);
- Education (over 50 educational institutions across 24 states); and
- Foreign government entities (United Arab Emirates' Sovereign Wealth Fund).[16]

[12] *Id.*
[13] *Id.*
[14] Jitendra Soni, *Clearview AI biometric firm suffers massive data breach*, https://www.techrader.com/news/clearview-ai-biometric-firm-suffers-massive-data-breach (last accessed Mar. 10, 2020).
[15] Caroline Haskins and Logan McDonald, *Clearview's Facial Recognition App Has Been Used by the Justice Department, ICE, Macy's, Walmart, and the NBA*, BuzzFeed News (Feb. 27, 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.
[16] *Id.*

36. The documents reviewed by BuzzFeed News indicate that the company has also provided its software to private investigators and security firms. Among them is Gavin de Becker and Associates, a private security agency that reportedly conducted thousands of searches, and SilverSeal, a New York private investigation and surveillance firm.[17]

37. Shockingly, the software was even provided to numerous wealthy or well-connected individuals who used Clearview for personal surveillance. According to *The New York Times*, billionaire John Catsimatidis was among the people given access to the app. [18] He surreptitiously snapped a picture of his daughter's date to research the date's biographical information, which he passed along to his daughter.[19] Peter Thiel, David Scalzo, Hal Lambert, and actor-turned-investor Ashton Kutcher were also listed in the report as either having access to or being suspected of having access to the app.[20]

38. The *Times* noted that Mr. Scalzo, the founder of the investment firm Kirenaga Partners, said in an interview that his school-aged daughters enjoyed playing with the app. "They like to use it on themselves and their friends to see who they look like in the world," he said. "It's kind of fun for people."[21]

39. In September, Ashton Kutcher described an app much like Clearview during a YouTube series called "Hot Ones," in which guests are interviewed while eating spicy chicken wings. "I have an app in my phone in my pocket right now. It's like a beta app," Mr. Kutcher said. "It's a facial recognition app. I can hold it up to anybody's face here and, like, find exactly who you are, what internet accounts you're on, what they look like. It's terrifying."[22]

[17] *Id.*
[18] Kashmir Hill, *Before Clearview Became a Police Tool, It Was a Secret Plaything of the Rich*, New York Times (Mar. 6, 2020), https://www.nytimes.com/2020/03/05/technology/clearview-investors.html.
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] *Id.*

40. In October 2019, Clearview asked Nicholas Cassimatis, an expert on artificial intelligence, to help conduct an internal accuracy test. He did the work for free, he said, because he knew Mr. Ton-That socially. The test consisted of submitting the faces of 834 federal and state legislators. Clearview's algorithms accurately identified every one of the politicians. After the test was complete, Mr. Cassimatis was allowed to keep Clearview's app on his phone. He said he had since run dozens of searches. "I tested it in surprising places: smoky bars, dark places. And it worked every time," Mr. Cassimatis said. "It's road testing. I do it as a hobby. I ask people for permission. It's like a parlor trick. People like it."[23]

41. Clearview has also shared its technology with organizations it designated as friends, conservative think tanks and lawmakers, and more than 20 potential investors around the world.[24]

42. Among the "friends" given access was SHW Partners LLC, a company founded by Jason Miller, a former Trump campaign senior communications official and one-time nominee for White House communications director.[25]

43. Clearview's data listed the offices of four members of Congress - including Rep. John Ratcliffe, a former nominee for the director of national intelligence - as having been given accounts, along with someone associated with the "White House Tech Office." That White House-affiliated account was credentialed in September 2019 and performed several searches.[26]

[23] *Id.*

[24] Ryan Mac, Caroline Haskins, and Logan McDonald, *Secret Users of Clearview AI's Facial Recognition Dragnet Included a Former Trump Staffer, a Troll, and Conservative Think Tanks*, BuzzFeed News (Mar. 11, 2020, updated Mar. 25, 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-trump-investors-friend-facial-recognition.

[25] *Id.*

[26] *Id.*

44. Beyond SHW, other entities on Clearview's list with the "Friend" designation included the Samarian Group, a New York-based private equity firm; Droese Raney, a Dallas commercial architecture company; and Clearview's outside counsel.[27]

45. Clearview's application is especially risky as law enforcement agencies are "uploading sensitive photos to the servers of a company whose ability to protect its data is untested."[28] Not only is it untested, but apparently is quite vulnerable as shown by the company's prior data breach.

CLEARVIEW'S DATA SECURITY IS WOEFULLY DEFICIENT

46. The importance of data security for companies storing biometric information is paramount because "facial recognition. . . cannot be changed."[29] "Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." 740 ILCS 14/5(c).

47. Despite the sensitivity of the information that Clearview stored, it did not maintain adequate security, as shown by its February 2020 data breach.[30]

[27] *Id.*
[28] Hill, *supra* n.1.
[29] Clare O'Gara, *What Are the Consequences of a Biometric Data Breach?*, Secure World Expo (Aug. 15, 2019), https://www.secureworldexpo.com/industry-news/biometric-data-breach-consequences.
[30] Alfred Ng, *Clearview AI's entire client list stolen in data breach*, C|Net (Feb. 26, 2020), https://www.cnet.com/news/clearview-ai-had-entire-client-list-stolen-in-data-breach/.

48. Clearview's inadequate security continues to be exposed—most recently a misconfigured server exposed the company's internal files, apps, and source code to anyone with an internet connection.[31]

49. That same data breach revealed some 70,000 videos in one of Clearview's cloud storage buckets, taken from a camera installed face-height in the lobby of a residential building.[32]

50. Clearview's co-founder Ton-That dismissed the myriad security concerns with the app by blaming individuals for posting their photos: "If it's public and it's out there and could be inside Google's search engine, it can be inside ours as well."[33] But Clearview crawls and obtains non-public photos and information that are well outside of "Google's search engine" and in violation of numerous companies' terms of service.

JURISDICTION AND VENUE

51. This Court has jurisdiction over this class action pursuant to 28 U.S.C. § 1332(d) because there are more than 100 class members and the aggregate amount in controversy exceeds $5,000,000, exclusive of interest, fees, and costs, and at least one class member is a citizen of a different state from one of the Defendants.

52. Venue is proper in this District under 28 U.S.C. § 1391 because Clearview maintains its corporate headquarters and principal place of business in this District.

PARTIES

53. Plaintiff Ryan Balfanz is a citizen and resident of San Francisco, California. Before 2017, Balfanz signed up for social media platforms, including Facebook. In so doing, he

[31] Zack Whittaker, *Security lapse exposed Clearview AI source code*, Tech Crunch (Apr. 16, 2020), https://techcrunch.com/2020/04/16/clearview-source-code-lapse/.
[32] *Id.*
[33] *Id.*

accepted Facebook's terms of service, which included an anti-scraping provision. Balfanz posted photographs to his Facebook account. Others have posted photographs of Balfanz on Facebook, as well. Balfanz never consented to third parties using the photographs he posted. Clearview never asked Balfanz for permission to use the photos he uploaded to Facebook, nor did Clearview compensate him for or notify him of its use of his photos. Balfanz would not have uploaded photos to Facebook had he known that Clearview would scrape and use his photographs for its dystopian facial recognition system. On information and belief, Mr. Balfanz's photos and personal information are stored in Clearview's servers without his consent.

54. Plaintiff Dean John is a citizen and resident of New York, New York. Before 2017, John signed up for social media platforms, including Facebook. In so doing, he accepted Facebook's terms of service, which included an anti-scraping provision. John posted photographs to his Facebook account. Others have posted photographs of John on Facebook, as well. John never consented to third parties using the photographs he posted. Clearview never asked John for permission to use the photos he uploaded to Facebook, nor did Clearview compensate him for or notify him of its use of his photos. John may not have uploaded photos to Facebook and other social media sites had he known that Clearview would scrape and use his photographs for its dystopian facial recognition system. On information and belief, Mr. John's photos and personal information are stored in Clearview's servers without his consent.

55. Plaintiff Benjamin Jais is a citizen and resident of Chicago, Illinois. Before 2017, Jais signed up for social media platforms, including Facebook. In so doing, he accepted Facebook's terms of service, which included an anti-scraping provision. Jais posted photographs to his Facebook account. Others have posted photographs of Jais on Facebook, as well. Jais never consented to third parties using the photographs he posted. Clearview never asked Jais for

permission to use the photos he uploaded to Facebook, nor did Clearview compensate him for or notify him of its use of his photos. Jais would not have uploaded photos to Facebook had he known that Clearview would scrape and use his photographs for its dystopian facial recognition system. On information and belief, Mr. Jais's photos and personal information are stored in Clearview's servers without his consent.

56. Plaintiff Rosemary Arias is a citizen and resident of Chicago, Illinois. Before 2017, Arias signed up for social media platforms, including Facebook. In so doing, she accepted Facebook's terms of service, which included an anti-scraping provision. Arias posted photographs to her Facebook account. Others have posted photographs of Arias on Facebook as well. Arias never consented to third parties using the photographs she posted. Clearview never asked Arias for permission to use the photos she uploaded to Facebook, nor did Clearview compensate her for or notify her of its use of her photos. Arias would not have uploaded photos to Facebook had she known that Clearview would scrape and use her photographs for its dystopian facial recognition system. On information and belief, Ms. Aria's photos and personal information are stored in Clearview's servers without her consent.

57. Plaintiff Aimee Albrecht is a citizen and resident of Alexis, Illinois. Before 2017, Albrecht signed up for social media platforms, including Facebook. In so doing, she accepted Facebook's terms of service, which included an anti-scraping provision. Albrecht posted photographs to her Facebook account. Others have posted photographs of Albrecht on Facebook as well. Albrecht never consented to third parties using the photographs she posted. Clearview never asked Albrecht for permission to use the photos she uploaded to Facebook, nor did Clearview compensate her for or notify her of its use of her photos. Albrecht would not have uploaded photos to Facebook had she known that Clearview would scrape and use her

photographs for its dystopian facial recognition system. On information and belief, Ms. Albrecht's photos and personal information are stored in Clearview's servers without her consent.

58. Defendant Clearview AI, Inc. is a Delaware corporation with its headquarters and principal place of business in the borough of Manhattan, New York, NY, 10091.

CLASS ACTION ALLEGATIONS

59. Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure 23(b)(2)-(3) and 23(c)(4) on behalf of themselves and the following Classes:

a. **Nationwide Class**: All individuals in the United States of America whose facial geometry was scanned by Clearview.

All Plaintiffs represent the Nationwide Class.

b. **Illinois Subclass**: All individuals in the State of Illinois whose facial geometry was scanned by Clearview.

Plaintiffs Jais, Arias, and Albrecht (the "Illinois Plaintiffs") represent the Illinois Subclass.

c. **New York Subclass**: All individuals in the State of New York whose facial geometry was scanned by Clearview.

Plaintiff John represents the New York Subclass.

d. **California Subclass**: All individuals in the State of California whose facial geometry was scanned by Clearview.

Plaintiff Balfanz represents the California Subclass.

60. **Numerosity:** The members of the Class and Subclasses are so numerous that individual joinder of all class members is impracticable. Based upon information and belief,

Plaintiffs believe that there are millions of class members affected by Clearview's unlawful practices.

61. **Commonality and Predominance:** This action involves common questions of law and fact, which predominate over any questions affecting individual class or subclass members, including:

a. Whether Clearview captured, collected, created, or otherwise obtained, stored, used, and commercialized; and disseminated or disclosed Plaintiffs' and the Classes' biometric identifiers or information;

b. Whether Clearview's actions violated state law;

c. Whether Clearview properly informed Plaintiffs and the Class that it was collecting, capturing, creating, or otherwise obtaining, storing, using, commercializing, and disseminating or disclosing their biometric identifiers or information;

d. Whether Clearview obtained a written release or consent from class members to engage in the practices as alleged herein;

e. Whether Clearview used Plaintiffs' and class members' biometric identifiers or biometric information to identify them;

f. Whether Clearview failed to develop a written policy for establishing the retention and deletion of biometric identifiers or biometric information, and whether Clearview's failure to disclose that policy to the public—if one existed—violated state law;

g. Whether Clearview acted negligently, recklessly, or intentionally in scraping individuals' photographs from the internet and using them to develop its software to identify individuals based upon facial geometry;

h. Whether Clearview should be enjoined from continuing its practices;

i. Whether Clearview failed to provide notice that it was scraping individuals' images from social media accounts;

j. Whether Clearview failed to provide notice that it was using, storing, and disseminating individuals' images, facial geometry, and biometric identifiers and/or information; and

k. Whether Clearview provided any mechanism for class members to consent to its practices.

62. **Typicality:** Plaintiffs' claims are typical of those of the other class members they seek to represent because, among other things, Plaintiffs and all class members were comparably injured through the uniform conduct described herein.

63. **Adequacy:** Plaintiffs are adequate representatives of the Classes because Plaintiffs' interests do not conflict with the interests of the other class members Plaintiffs seek to represent; Plaintiffs have retained counsel competent and experienced in complex commercial and class action litigation; and Plaintiffs intend to prosecute this action vigorously. The interests of the class members will be fairly and adequately protected by Plaintiffs and their counsel.

64. **Declaratory and Injunctive Relief:** Defendants have acted or refused to act on grounds generally applicable to Plaintiffs and the other class members, thereby making appropriate final injunctive relief and declaratory relief, as described below, with respect to class members as a whole.

65. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the other class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Clearview, making it impracticable for class members to individually seek redress for Clearview's wrongful conduct. Even if class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION
On behalf of the Illinois Subclass
Illinois Biometric Privacy Act, 740 ILCS 14/1, *et seq.*

66. The Illinois Plaintiffs reallege and incorporate by reference paragraphs 1 through 58 as though set forth herein.

67. According to the Illinois Biometric Privacy Act, "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." 740 ILCS 14/5(c).

68. Biometric information is “any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual.” 740 ILCS 14/10. Scans of an individual’s face geometry are a type of “biometric identifier.” 740 ILCS 14/10.

69. Pursuant to BIPA, “[a] private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.” 740 ILCS 14/10(a).

70. In accordance with BIPA, “[n]o private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person’s or a customer’s biometric identifier or biometric information unless it first: (1) informs the subject or the subject’s legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject or the subject’s legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject’s legally authored representative.” 740 ILCS 14/15(b).

71. Additionally, “[n]o private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person’s. . . biometric identifier or biometric information.” 740 ILCS 14/15(c).

72. Further, "[n]o private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's. . . biometric identifier or biometric information unless: (1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure; (2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information of the subject's legally authorized representative; (3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or (4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction." 740 ILCS 14/15(d).

73. Finally, "[a] private entity in possession of a biometric identifier or biometric information shall: (1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and (2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information." 740 ILCS 14/15(e).

74. BIPA provides for a private right of action and allows a prevailing party to recover liquidated damages in the amount of: (a) $1,000 or actual damages, whichever is greater for negligent violations of its provisions; and (b) $5,000 or actual damages, whichever is greater, for intentional or reckless violations of its provisions. 740 ILCS 14/20. BIPA also allows for the recovery of attorneys' fees and costs and injunctive relief. 740 ILCS 14/20.

75. Despite the clear language of the statute, Clearview secretly created a database of over three billion facial images—including those of individuals in Illinois—to support its secret facial recognition application that it marketed to private companies and law enforcement.

76. Clearview AI subjects each image it scrapes from the internet to Clearview AI's "state-of-the-art neural net" facial scanning technology. Clearview AI explains the process as converting an individual's face geometry "into mathematical formulas, or vectors, *based on facial geometry* — like how apart a person's eyes are." Clearview AI then groups similar facial geometry-based vectors (*i.e.* vectors of the same face but in different photographs) together into "neighborhoods" within its database.

77. Every Illinois citizen pictured in images scraped by Clearview AI had his or her face geometry scanned, converted into a mathematical formula, and stored in Clearview AI's database.

78. The vectors Clearview AI creates are biometric identifiers that Clearview AI uses to identify individuals in images uploaded to Clearview AI's database based upon their face geometry—accordingly, Clearview has engaged, and continues to engage in, the precise conduct BIPA regulates.

79. Clearview intentionally and recklessly scraped these images, collected and stored biometric information, disclosed that biometric information, and profited off that biometric information without any disclosure, notice, or consent from the individuals whose images it scraped.

80. Clearview purposefully has avoided providing notices or obtaining consent from the Illinois individuals in its database in order to ensure that its database is as comprehensive as possible.

81. Until late 2019, Clearview's website (https://clearview.ai) contained only the statement "Artificial Intelligence for a better world," and a clickable button that read "REQUEST ACCESS" with an address in New York City—Clearview did not provide the public with a clear written policy of the retention of this information, or when that information would be destroyed.

82. In violation of BIPA, Defendants collected, captured and otherwise obtained individuals' biometric identifiers and information — including, on information and belief, the biometric identifiers and information of the Illinois Plaintiffs and Illinois Class members — without providing the requisite written information and without obtaining the requisite written releases.

83. In violation of BIPA, Clearview sold, leased, traded and otherwise profited from individuals' biometric identifiers and information, including the biometric identifiers and information of the Illinois Plaintiffs and Illinois Class members. As detailed herein, Clearview provided this data to numerous entities and individuals unaffiliated with law enforcement.

84. In violation of BIPA, Clearview disclosed, redisclosed and otherwise disseminated individuals' biometric identifiers and information, including the biometric identifiers and information of the Illinois Plaintiffs and Illinois Class members, even though: (a) neither the subjects of the biometric identifiers and information nor their authorized representatives consented to the disclosure or redisclosure; (b) the disclosure or redisclosure did not complete a financial transaction requested or authorized by the subjects of the biometric identifiers and information or their authorized representatives; (c) the disclosure or redisclosure was not required by State or federal law or municipal ordinance; and (d) the disclosure was not required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

85. In violation of BIPA, Clearview did not develop a written policy that they made available to the public that established a retention schedule and guidelines for permanently destroying biometric identifiers and information.

86. As a result of Clearview's intentional and/or reckless violation of BIPA, the Illinois Plaintiffs and Illinois Class members already have been injured and will continue to be injured, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
On behalf of the California Subclass
Cal. Bus. & Prof. Code § 17200, *et seq.*

87. Plaintiff Balfanz realleges and incorporates by reference paragraphs 1 through 58 as though set forth herein.

88. Clearview violated California's Unfair Competition Law (UCL), Cal. Bus. & Prof. Code § 17200, *et seq.*, by engaging in the unlawful and unfair business acts and practices alleged previously and as further specified below.

89. Clearview's theft and use of photographs posted to various social networking platforms for profit, without authorization from or compensation paid to the individuals in the photographs or the photographs' owners, is unethical, unscrupulous, and substantially injurious to Plaintiffs and class members, and thus constitutes an unfair practice under the UCL. The following are examples of Clearview's unfair business practices:

a. Scraping billions of photographs without the consent of their owners, many of which had been uploaded subject to Terms of Service of websites which limited how they could be used;

b. Invading the privacy of consumers;

c. Failing to provide adequate data security of the data it has collected;

d. Exposing consumers' sensitive personal data to theft by foreign actors and criminals;

e. Violating the rights that consumers have as to the display and distribution of their photographs and other property rights;

f. Exposing consumers to the threat of surveillance, stalking, harassing, and fraud; and

g. Profiting from use of these unfairly obtained photographs.

90. Clearview's practices are also contrary to legislatively declared and public policies that seek to protect consumers from unauthorized use of their data, as reflected in laws like the California Consumer Privacy Act of 2018 (Cal. Civ. Code § 1798.100, *et seq.*) California's Right of Publicity statute (Cal. Civ. Code § 3344), and the California Constitution's Right of Privacy (Article 1, Section 1). The harm these practices caused to Plaintiffs and class members outweighs any utility of these practices.

91. Clearview knew or should have known that it was collecting and using photographs whose owners and/or subjects did not authorize their collection or use, and whose photograph-hosting platforms did not authorize their collection or use. This unauthorized collection and use gave Clearview an unfair competitive advantage, as these photographs provided the data for Clearview's facial recognition software, from which it profits.

92. Clearview's business practices also constitute unlawful practices under the UCL, as they violate the following:

a. 18 U.S.C. § 1030(a)(2) & (c), which prohibits "intentionally access[ing] a computer without authorization," and thereby obtaining "information from any protected computer";

b. California Penal Code § 502(c)(1), which prohibits persons from "[k]knowingly access[ing] and without permission . . . us[ing] any data, computer, computer system, or computer network in order to . . . wrongfully control or obtain . . . data";

c. California Penal Code § 502(c)(2), which prohibits persons from "[k]knowingly access[ing] and without permission tak[ing], cop[ying], or mak[ing] use of any data from a computer, computer system, or computer network; and

d. Cal. Civ. Code § 3344, which prohibits "knowingly" using "another's . . . photograph, or likeness, In any manner, on or in products . . . without such person's prior consent."

93. Plaintiffs have standing to bring these claims under the UCL because Clearview was unjustly enriched and Plaintiffs were injured and lost money or property, including but not limited to the value of their likenesses for which, as a result of Clearview's unlawful and unfair business practices, they were not compensated. Clearview's actions demonstrate that Plaintiffs' data was valuable to Clearview, or else they would not have made efforts to obtain it. Further, Plaintiffs and class members have an interest in controlling the use of their identities, names, and likenesses. Among other things, Plaintiffs may have used social media differently had they known that a third party could use their photographs and personal data without permission.

94. Pursuant to California Business and Professions Code § 17203, Plaintiffs seek equitable relief to prevent the continuation of Clearview's unfair and unlawful practices.

THIRD CAUSE OF ACTION
California Common Law Right of Publicity
On behalf of the California Subclass

95. Plaintiff Balfanz realleges and incorporates by reference paragraphs 1 through 58 as though set forth herein.

96. California's common law right of publicity protects persons from authorized use of a person's identity by another for commercial gain.

97. Clearview knowingly used the identities, photographs, and likenesses of Plaintiffs and class members to create a facial recognition software product, from which Clearview profits.

98. Clearview did not have the consent of Plaintiffs or class members to do so.

99. Plaintiffs were harmed by Clearview's actions, including by Clearview's failure to compensate Plaintiffs for use of their identities and photographs.

100. Use of Plaintiffs' identities, photographs, and likenesses was directly connected to Clearview's commercial activity.

101. Clearview's actions were a substantial factor in causing Plaintiffs harm.

102. As a direct and proximate result of Clearview's misconduct, Plaintiffs and class members have suffered damage and are entitled to monetary damages in an amount to be determined at trial. Plaintiffs and class members also seek injunctive relief, and such other equitable or declaratory relief as may be appropriate.

FOURTH CAUSE OF ACTION
California Constitutional Right to Privacy
On behalf of the California Subclass

103. Plaintiff Balfanz realleges and incorporates by reference paragraphs 1 through 58 as though set forth herein.

104. Plaintiffs possess legally protected privacy interests, including but not limited to conducting personal activities without intrusion or interference. Plaintiffs' privacy in their personal data, photographs, identities, likenesses, and social engagements are reflected in several laws, including the California Consumer Privacy Act of 2018 (Cal. Civ. Code § 1798.100, et seq.) California's Right of Publicity statute (Cal. Civ. Code § 3344), and California's common law right of publicity.

105. Plaintiffs expected that their personal data, photographs, and likenesses would not be scraped to create robust facial recognition software without their consent. This expectation was reasonable, as several social media platforms' terms of service and issuance of cease-and-desist letters demonstrates.

106. Clearview intruded into Plaintiffs' privacy rights by scraping their photographs and photographs of them without their consent and using their data and identities to build robust facial recognition technology.

107. These intrusions were so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of social norms.

108. As a result of Clearview's privacy intrusions, Plaintiffs and class members were injured. Plaintiffs thus request injunctive relief and damages in an amount to be determined at trial.

FIFTH CAUSE OF ACTION
Intentional Interference with Contractual Relations
On behalf of the National Class and Each of the Subclasses

109. Plaintiffs reallege and incorporate by reference paragraphs 1 through 58 as though set forth herein.

110. Plaintiffs used and uploaded photographs to social media platforms, including Facebook and others. They entered into contracts with those social media platforms (terms of service) that governed Plaintiffs' use of those platforms, and in turn those platforms' use of Plaintiffs' uploaded content. Those terms of service stated that Plaintiffs' data would not be scraped from the platform.

111. As a sophisticated technology company, Clearview knew that individuals use social media platforms subject to terms of service that prohibit third party scraping. Clearview was thus well aware of these terms of service.

112. Clearview intentionally scraped Plaintiffs' photographs and data from these social media platforms, in direct contravention of the terms of service contracts entered into by Plaintiffs with these social media platforms.

113. Clearview caused an actual breach or disruption of Plaintiffs' contractual relationship with social media platforms. For example, Plaintiffs' data was actually scraped, despite prohibitions of scraping in social media platforms' terms of service.

114. As a result, Plaintiffs suffered damages, including but not limited to loss of control of their likenesses and photographs. Plaintiffs and class members are entitled to monetary damages in an amount to be determined at trial.

SIXTH CAUSE OF ACTION
Unjust Enrichment
On behalf of the National Class and Each of the Subclasses

115. Plaintiffs reallege and incorporate by reference paragraphs 1 through 58 as though set forth herein.

116. To the detriment of Plaintiffs and class members, Defendant has been, and continues to be, unjustly enriched as a result of its wrongful conduct alleged herein.

117. Plaintiffs and class members conferred a benefit on Defendant when Defendant scraped their photographs and other indicia of their identities from social media platforms without their consent or compensation.

118. Defendant profited from this data at Plaintiffs' and class members' expense by creating and selling its facial recognition software, which could not have occurred without wrongfully obtaining Plaintiffs' and class members' photographs.

119. Under the circumstances, it would be unjust and inequitable to allow Defendant to retain these profits without compensating Plaintiffs and class members. Equity and good conscience require restitution.

120. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein.

Plaintiffs and class members, therefore, seek compensation for all their photographs and data that Defendant wrongfully obtained as a result of its inequitable conduct as more fully stated herein.

PRAYER FOR RELIEF

Plaintiffs respectfully request that the Court enter judgment in their favor, and against Clearview, as follows:

a. That the Court certify the Classes, name Plaintiffs as Class Representatives, and appoint their lawyers as Class Counsel;

b. That the Court grant permanent injunctive relief to prohibit Clearview from continuing to engage in the unlawful acts and practices described herein;

c. That the Court award Plaintiffs and the other members of the Classes statutory, compensatory, consequential, general, and nominal damages in an amount to be determined at trial;

d. That the Court award punitive or exemplary damages in an amount to be determined at trial;

e. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

f. That the Court award pre- and post-judgment interest at the maximum legal rate; and

g. That the Court grant all such other relief as it deems just and proper.

JURY DEMAND

Plaintiffs demand a trial by jury on all claims so triable.

Dated: May 4, 2020 Respectfully submitted,

/s/ Scott Martin
Scott Martin (NY Bar No.: 2387843)
Steven M. Nathan (NY Bar No.: 2156289)
HAUSFELD LLP
33 Whitehall St., 14th Floor
New York, NY 10004
Tel: (646) 357-1100
smartin@hausfeld.com
snathan@hausfeld.com

James J. Pizzirusso
HAUSFELD LLP
1700 K St., NW, Ste 650
Washington, DC 20006
Telephone: 202-540-7200
Facsimile: 202-540-7201
jpizzirusso@hausfeld.com

Greg G. Gutzler
DICELLO LEVITT GUTZLER LLC
444 Madison Avenue, Fourth Floor
New York, NY 10022
Tel.: 646-933-1000
ggutzler@dicellolevitt.com

Adam J. Levitt
Amy E. Keller
DICELLO LEVITT GUTZLER LLC
Ten North Dearborn Street, Sixth Floor
Chicago, IL 60602
Tel.: 312-214-7900
alevitt@dicellolevitt.com
akeller@dicellolevitt.com

Eric H. Gibbs
David M. Berger
GIBBS LAW GROUP LLP
505 14th Street, Suite 1110
Oakland, CA 94611
Tel.: 510-350-9713
ehg@classlawgroup.com
dmb@classlawgroup.com