

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK**

MARIO CALDERON and JENNIFER ROCIO,
individually and on behalf of all others similarly
situated,

Plaintiffs,

v.

CLEARVIEW AI, INC. and
CDW GOVERNMENT LLC,

Defendants.

Civil Action No.:

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs Mario Calderon and Jennifer Rocio (“Plaintiffs”) bring this Class Action Complaint against Defendants Clearview AI, Inc. (“Clearview”) and CDW Government LLC (“CDW”) or (collectively “Defendants”), individually and on behalf of all others similarly situated, and complain and allege upon personal knowledge as to themselves and their own acts and experiences and, as to all other matters, upon information and belief, including an investigation conducted by their attorneys:

NATURE OF THE ACTION

1. Plaintiffs bring this action for damages and other legal and equitable remedies resulting from the illegal actions of Clearview and CDW in collecting, storing and using their and other similarly situated individuals’ biometric identifiers¹ and biometric information² (referred to collectively at times as “biometrics”) without informed written consent, in direct

¹ A “biometric identifier” is any personal feature that is unique to an individual, including fingerprints, iris scans, DNA and “face geometry,” among others.

² “Biometric information” is any information captured, converted, stored, or shared based on a person’s biometric identifier used to identify an individual.

violation of Illinois' Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, *et seq.*

2. The Illinois Legislature has found that "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information." 740 ILCS 14/5(c). "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." *Id.*

3. In recognition of these concerns over the security of individuals' biometrics, the Illinois Legislature enacted BIPA, which provides, *inter alia*, that a private entity like Clearview may not obtain and/or possess an individual's biometrics unless it: (1) informs that person in writing that biometric identifiers or information will be collected or stored; (2) informs that person in writing of the specific purpose and length of term for which such biometric identifiers or biometric information is being collected, stored and used; (3) receives a written release from the person for the collection of her or her biometric identifiers or information; and (4) publishes publicly available written retention schedules and guidelines for permanently destroying biometric identifiers and biometric information.

4. In direct violation of each of the foregoing provisions, Clearview and CDW actively collected, stored and used Plaintiffs' biometrics—and the biometrics of most of the residents of Illinois—without providing notice, obtaining informed written consent or publishing data retention policies.

5. Specifically, Clearview has amassed a database of more than three billion photographs that it scraped from sources including Instagram, Twitter, YouTube, Facebook, Venmo and millions of other websites. Using this data, Clearview created a facial recognition

tool that can identify virtually anyone by simply uploading a photograph. Users can take a picture of a stranger on the street, upload it to Clearview's tool and instantly see photos of that person on various social media platforms and websites, along with the person's name, address and other identifying information.

6. As the New York Times explained, this tool, which Clearview has licensed to "hundreds of law enforcement agencies," could "end your ability to walk down the street anonymously." "The weaponization possibilities of this are endless," said Eric Goldman, co-director of the High Tech Law Institute at Santa Clara University. "Imagine a rogue law enforcement officer who wants to stalk potential romantic partners, or a foreign government using this to dig up secrets about people to blackmail them or throw them in jail."

7. Clearview sells its facial recognition tool through its Illinois-based agent CDW. CDW, on behalf of Clearview, licenses the Clearview app to law enforcement agencies and other entities. One of Clearview's clients, obtained through CDW, is the Chicago Police Department ("CPD"). The CPD entered into a two-year, \$49,875 contract on January 1, 2020 with CDW to use Clearview's technology. For at least two months before that, select officials at the CPD's Crime Prevention and Information Center ("CPIC") used the software on a trial basis after another law enforcement agency recommended the technology. After the trial ended, the CPD was so impressed with the results that it gave approximately 30 CPIC officials full access to Clearview's technology, effectively unleashing this vast, Orwellian surveillance tool on the citizens of Illinois.

JURISDICTION AND VENUE

8. This Court has original jurisdiction over this controversy pursuant to 28 U.S.C. § 1332(d) because there are more than 100 class members and the aggregate amount in

controversy exceeds \$5,000,000.00, exclusive of interest, fees, and costs, and at least one Class member is a citizen of a state different from one of the Defendants.

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

PARTIES

10. Plaintiff Mario Calderon is, and has been at all relevant times, a resident and citizen of Chicago, Illinois. Mr. Calderon is an account holder for several services from which Clearview has scraped data, including Facebook, Instagram, Snapchat and Google Photos. He has uploaded photographs depicting his face to these websites from within Illinois on a regular basis, at least some of which are publicly available. These photographs contained metadata reflecting that he was located within Illinois. As such, Mr. Calderon is informed and believes that his biometrics (a scan of facial geometry) are contained in Clearview's database and that his biometrics have been disclosed to CDW and CPD and used by CDW and CPD via Clearview's proprietary platform. Defendants' collection, storage and use of his biometrics violated Mr. Calderon's statutorily protected rights under BIPA. Defendants' actions also invaded his privacy and caused him to lose control over his biometrics.

11. Plaintiff Jennifer Rocio is, and has been at all relevant times, a resident and citizen of Romeoville, Illinois. Ms. Rocio is an account holder for several services from which, on information and belief, Clearview has scraped data, including Facebook, Snapchat, Instagram, YouTube, TikTok and others. She has uploaded photographs depicting her face to these websites from within Illinois on a regular basis, at least some of which are publicly available. These photographs contained metadata reflecting that she was located within Illinois. As such, Ms. Rocio is informed and believes that her biometrics (a scan of facial geometry) are contained

in Clearview's database and that her biometrics have been disclosed to CDW and CPD and used by CDW and CPD via Clearview's proprietary platform. Defendants' collection, storage and use of her biometrics violated her statutorily protected rights under BIPA. Defendants' actions also invaded her privacy and caused her to lose control over her biometrics.

12. Defendant Clearview AI, Inc. is a Delaware corporation with its headquarters located at 214 W 29th Street, 2nd Floor, New York, NY, 10001. Clearview has collected the biometrics of Illinois residents without the requisite consent, including that of the Plaintiffs and members of the proposed Class, and has sold or otherwise disclosed that data to Illinois-based entities, including to the Chicago Police Department. Clearview continues to engage in this conduct to this day.

13. Defendant CDW Government LLC is an Illinois company headquartered in Vernon Hills, Illinois. CDW acts as Clearview's agent to license Clearview's proprietary facial recognition platform to third parties, including the Chicago Police Department.

CLASS ACTION ALLEGATIONS

14. Plaintiff seeks to represent a class defined as all individuals who, while residing in the state of Illinois, had their biometric identifiers captured, collected, or obtained by Clearview at any point during the preceding five years. Excluded from the Class is any entity in which any Defendant has a controlling interest, and officers or directors of Defendants.

15. Members of the Class are so numerous that their individual joinder herein is impracticable. Upon information and belief, members of the Class number in the millions. The precise number of Class members and their identities are unknown to Plaintiffs at this time but may be determined through discovery. Class members may be notified of the pendency of this action by mail and/or publication through the distribution records of Defendants.

16. Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Common legal and factual questions include, but are not limited to:

- a. whether Defendants properly informed Plaintiffs and each Class member that they collected, used, and stored their biometric identifiers or biometric information;
- b. whether Defendants obtained a written release (as defined in 740 ILCS 1410) to collect, use, and store Plaintiffs' and each Class member's biometric identifiers or biometric information;
- c. whether Defendants violated BIPA in Illinois by collecting, capturing, or obtaining Plaintiffs' and each Class member's biometric identifiers or biometric information absent the requisite informed written release;
- d. whether Defendants developed 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 their last interaction, whichever occurs first;
- e. whether Defendants stored, disclosed, sold, or otherwise used Plaintiffs' and each Class's biometric identifiers or biometric information in Illinois;
- f. whether any violations of BIPA committed by Defendants were committed negligently; and
- g. whether any violations of BIPA committed by Defendants were committed knowingly or recklessly.

17. The claims of the named Plaintiffs are typical of the claims of the Class in that Defendants collected, captured, or obtained each of their biometrics while each was residing in Illinois, without obtaining consent or adhering to the other requirements of BIPA.

18. Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the Class members they seek to represent, they have retained competent counsel experienced in prosecuting class actions, and they intend to prosecute this action vigorously. The interests of Class members will be fairly and adequately protected by Plaintiffs and their counsel.

19. The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of Class members. Each individual Class member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendants' liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendants' liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

COUNT I
Violation of the Illinois Biometric Information
Privacy Act, 740 ILCS 14/1, *et seq.*

20. Plaintiffs incorporate by reference the foregoing allegations as if fully set forth herein.

21. Illinois' BIPA requires private entities, such as Defendants, to obtain informed written consent from individuals before acquiring their biometric information. Specifically, BIPA makes it unlawful to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or customer's biometric identifiers or biometric information unless [the entity] first: (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of for which a biometric identifier or biometric information is being captured, collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or

biometric information” 740 ILCS 14/15(b).

22. Illinois’ BIPA also requires that private entities in possession of biometric identifiers and/or biometric information establish and maintain a publicly available retention policy. Entities which possess biometric identifiers or information must (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric information (entities may not retain biometric information longer than three years after the last interaction with the individual); and (ii) must adhere to the publicly posted retention and deletion schedule.

23. Defendants are each a “private entity” as that term is defined under BIPA. *See* 740 ILCS 14/10.

24. Plaintiffs are informed and believe that, through photographs available on various websites, Defendants collected, captured, received or otherwise obtained the “biometric identifiers” of Plaintiffs and the other Class members, including scans of their face geometry.

25. Using data derived from Plaintiffs’ and the Class members’ biometric identifiers, Plaintiffs are informed and believe that Defendants also collected, captured, received or otherwise obtained the “biometric information” of Plaintiffs and the other Class members, in the form of their name, gender, age, location and other data.

26. Plaintiffs are informed and believe that Defendants thereafter sold or otherwise disclosed Plaintiffs’ and the other Class members’ biometric identifiers and/or biometric information to other third parties in Illinois. Plaintiffs are informed and believe that one or more of these third parties, by way of Clearview’s platform, used and stored Plaintiffs’ and the other Class members’ biometrics in Illinois.

27. Defendants’ practices with respect to capturing, collecting, storing, and using

biometric identifiers and biometric information fails to comply with applicable BIPA requirements. Specifically, with respect to Plaintiffs and the other Class members, Defendants failed to:

- a. obtain the written release required by 740 ILCS 14/15(b)(3);
- b. inform Plaintiffs and the other Class members in writing that their biometric identifiers and/or biometric information were being captured, collected, stored, and used, as required by 740 ILCS 14/15(b)(1);
- c. inform Plaintiffs and the other Class members in writing of the specific purpose for which their biometric information and/or biometric identifiers were being captured, collected, stored, and used, as required by 740 ILCS 14/15(b)(2);
- d. inform Plaintiffs and the other Class members in writing of the specific length of term their biometric information and/or biometric identifiers were being captured, collected, stored and used, as required by 740 ILCS 14/15(b)(2); and
- e. provide a publicly available retention schedule detailing the length of time biometric information is stored and guidelines for permanently destroying the biometric information it stores, as required by 740 ILCS 14/15(a).

28. By capturing, collecting, storing, and using Plaintiffs' and the other Class members' biometric identifiers and/or biometric information as described herein, Defendants violated Plaintiffs' and the other Class members' respective rights to privacy as set forth in BIPA. 740 ILCS 14/15(a).

29. BIPA provides for statutory damages of \$5,000 for each willful and/or reckless violation of BIPA and, alternatively, damages of \$1,000 for each negligent violation of BIPA. 740 ILCS 14/20(1).

30. The harms suffered by the Plaintiffs and other members of the Class are actual injuries, compensable in actual monetary damages under BIPA, no different than any other non-pecuniary yet monetarily compensable injuries (e.g., reputational harm, pain and suffering, mental and emotional distress, loss of consortium, and the list goes on and on).

31. Defendants' violations of BIPA, as set forth herein, were knowing and willful, or

were in reckless disregard of the statutory requirements. Alternatively, Defendants negligently failed to comply with BIPA disclosure, consent, and policy posting requirements.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the other Class members respectfully request that the Court:

- a. Certify the Class as defined above, appointing Plaintiffs as class representatives and the undersigned as class counsel;
- b. Declare that Defendants' actions, as set forth herein, violate BIPA;
- c. Award injunctive and equitable relief as necessary to protect the interests of Plaintiffs and the Class by requiring Defendants to comply with BIPA requirements for the capture, collection, storage, and use of biometric identifiers and biometric information, including an injunction requiring Defendants to permanently destroy all biometric information of Plaintiffs and the other Class members in their possession and compensation in an amount to be determined at trial for the commercial value of Plaintiff's biometric information;
- d. Award statutory damages of \$5,000 for each willful and/or reckless violation of the BIPA, pursuant to 740 ILCS 14/20(1);
- e. Award statutory damages of \$1,000 for each negligent violation of BIPA, pursuant to 740 ILCS 14/20(3);
- f. Award reasonable attorneys' fees, costs, and other litigation expenses pursuant to 740 ILCS 14/20(3);
- g. Award pre- and post-judgment interest, as allowable by law; and
- h. Award such further and other relief as the Court deems just and equitable.

JURY DEMAND

Plaintiffs demand a trial by jury on all causes of action and issues so triable.

Dated: February 13, 2020

Respectfully submitted,

BURSOR & FISHER, P.A.

By: /s/ Joshua D. Arisohn
Joshua D. Arisohn

Scott A. Bursor
Joshua D. Arisohn
888 Seventh Avenue
New York, NY 10019
Tel: (646) 837-7150
Fax: (212) 989-9163
E-Mail: scott@bursor.com
jarisohn@bursor.com

Frank S. Hedin (to be admitted *pro hac vice*)
HEDIN HALL LLP
Four Embarcadero Center, Suite 1400
San Francisco, California 94104
Telephone: (415) 766-3534
Facsimile: (415) 402-0058
Email: fhedin@hedinhall.com

Attorneys for Plaintiffs