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 identifiers[1] and biometric information[2] (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 is 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.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.