IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

ANTHONY HALL, on behalf of himself and all others similarly situated,	)	
Plaintiff,	)	
	)	Case No. 20-cv-00846
vs.	)	
CLEARVIEW AI, INC., and. CDW GOVERNMENT LLC;	)	Jury Demanded
Defendants.	)	

CLASS ACTION COMPLAINT

Plaintiff Anthony Hall, on behalf of himself and a putative class ("Plaintiff" or "Hall"), brings this Class Action Complaint against Defendants Clearview AI, Inc ("Clearview"); CDW Government, LLC ("CDW") and alleges the following:

Introduction

1. A New York Times article published on January 18, 2020 introduced Americans to the then relatively unknown company Clearview AI, Inc. The article described a dystopian surveillance database, owned and operated by a private company and leased to the highest bidder.

2. Clearview AI's database includes the photographs, and personal and private data, including names, home addresses, and work addresses, of millions of Americans. Clearview acquired the billions of data points by "scraping" or harvesting the data from publicly available internet-based platforms such as Facebook, Instagram, and Twitter.

3. But Clearview's database is unique – it has run every one of the 3 billion photographs it has acquired through facial recognition software to extract and index the unique biometric data from each face. The database thus also contains the biometric identifiers and information of millions of Americans. Any private citizen can be identified by uploading a photo to the database. Once identified, the end-user then has access to all of the individual's personal details that Clearview has also obtained.

4. A second article published in the Chicago Sun-Times on January 29, 2020 revealed that the Chicago Police Department was using Clearview's surveillance database to aid in law enforcement operations.

Jurisdiction

5. This Court has jurisdiction under 28 U.S.C. § 1332(d)(2), the Class Action Fairness Act ("CAFA") because there are 100 or more members of the class, the parties and putative class members are minimally diverse and the aggregate amount in controversy is greater than $5,000,000.

6. This Court has personal jurisdiction over Clearview because they conduct a substantial amount of business here which forms the basis of Plaintiffs' claims. Clearview has made their surveillance database, which contains the private and personal data and biometric information of thousands of Illinois residents, available to Chicago Police department. All defendants' violations of Illinois law are based on and arise from their contacts with the state and its residents. The court has personal jurisdiction over CDW because they are an Illinois company headquartered in Illinois.

7. Venue is proper here under 28 U.S.C. § 1391(b)(2) because a substantial amount of the acts and omissions giving rise to the claims occurred in Illinois.

Parties

8. Anthony Hall is a natural person and resident of this district. He maintains an active presence on social media, including Facebook and Instagram. He also uses Venmo to make and accept payments to other individuals.

9. Clearview AI, Inc. is a Delaware corporation with its headquarters in New York City, New York. It owns and operates the surveillance database and markets its products to Illinois-based companies and agencies, including the Chicago Police Department.

10. CDW Government LLC ("CDW"), is an Illinois company headquartered in Vernon Hills, Illinois. CDW provides equipment and services to local government agencies, including the Chicago Police Department.

Clearview's Surveillance Database

11. Clearview 'scrapes,' 'harvests,' or otherwise obtains information and photos of millions of Americans from the internet, in particular social media platforms like Facebook and Instagram. That is, they use automated software or processes to obtain massive amounts of data without the consent or knowledge of the platform users.

12. Clearview then runs the photos through facial recognition software which identifies the photos that contain faces.

13. The faces are then processed by Clearview's software, and their biometric data is extracted. The biometric data is a collection of vectors and/or other data points that allows faces to be classified, searched and indexed.

14. Clearview's database links the biometric data to the other data Clearview has scraped so an end-user can find out where the photos came from along with a significant amount of personal and private details about a given individual.

15. In short, anyone with access to the database, including any employee of Clearview, or reseller of the database, or end-user can upload a single photo and identify the person in real-time. A single picture on the internet means that any private citizen can immediately be identified and tracked.

16. Clearview sells or leases access to the surveillance database to public and private entities for profit.

17. Clearview also contracts with third parties, for example CDW, to sell or lease access to the surveillance database.

18. Clearview offers 30-day free trials to individual law enforcement officers so that they will encourage their departments to subscribe to the database.

19. Clearview also monitors the use of the database by the end-users – Clearview employees can see who law enforcement officers are searching for.

The Illinois Biometric Information Privacy Act ("BIPA")

20. More than ten years ago, the Illinois Legislature recognized the promises and perils of biometric identification technology. It passed the Biometric Information Privacy Act, 740 ILCS § 14/1 *et seq.*, to establish and safeguard Illinois' residents absolute right to control their biometric data.

21. BIPA regulates both biometric identifiers and biometric information. *See, id.*

22. Under the act, a "scan of…face geometry," is a biometric identifier. *Id.* at § 14/10.

23. Biometric information is any information derived from a biometric identifier. *Id.*

24. Under the act, a private entity like Clearview or CDW in possession of either biometric identifiers or information must develop a written policy, available to the public, establishing a retention schedule and guidelines for permanently destroying the information or identifiers. *Id.* § 14/15(a).

25. Clearview and CDW are in possession of biometric identifiers and information which is stored in the Clearview database.

26. Neither Defendant has provided any policy whatsoever establishing either a retention schedule or guidelines for permanently destroying the biometric data.

27. Under the act, a private entity like Clearview or CDW is prohibited from collecting, capturing, or otherwise obtaining a person's biometric information or identifier unless it first: a) informs the subject in writing that the information or identifier is being collected or stored; b) informs the subject in writing of the specific purpose and length of term for which the information or identifier is being collected, stored, or used;, and, c) receives a written release from the subject of the information or identifier. *Id.* at § 14/15(b).

28. Neither Clearview nor CDW at any relevant time had informed Plaintiff or any member of the Class (described below) any of the information required under § 14/15(b). Neither the Plaintiff nor members of the putative Class executed a written release to Clearview or CDW.

29. Under the act, a private entity, like Clearview or CDW, in possession of a person's biometric identifier or information may not sell, lease, trade, or otherwise, profit from a person's information or identifier. *Id.* § 14/15(c).

30. Clearview and CDW are actively selling and/or leasing and profiting off the Plaintiff's and each member of the putative class' information or identifier. They have multiple contracts across the country, including Illinois, to provide access to the surveillance database for money.

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.