

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

In re Clearview AI, Inc., Consumer Privacy
Litigation

This document relates to:

All actions

Civil Action File No.: 1:21-cv-00135

Judge Sharon Johnson Coleman

Magistrate Judge Maria Valdez

JURY TRIAL DEMANDED

SECOND AMENDED CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs David Mutnick, Steven Vance, Mario Calderon, Anthony Hall, Isela Carmean, Shelby Zelonis Roberson, Andrea Vestrand and Aaron Hurvitz (collectively, “Plaintiffs”), individually and on behalf of all others similarly situated (“Plaintiff Class Members”), bring this Second Amended Consolidated Class Action Complaint against the following: (a) Clearview AI, Inc., formerly known as Smartcheckr Corp., Inc. (“Clearview”); (b) Hoan Ton-That; (c) Richard Schwartz; (d) Rocky Mountain Data Analytics LLC (“Rocky Mountain”); (e) Thomas Mulcaire; and (f) Macy’s, Inc. (“Macy’s”); (g) Macy’s Retail Holdings, Inc., now known as Macy’s Retail Holdings, LLC; (h) Macy’s Corporate Services, Inc., now known as Macy’s Corporate Services, LLC; (i) AT&T Inc. (“AT&T”); (j) Kohl’s, Inc. (“Kohl’s”); (k) Best Buy Stores, L.P. (“Best Buy”); (l) Albertsons Companies, LLC (“Albertsons”); (m) Walmart Inc. (“Walmart”); and (n) The Home Depot, Inc. (“Home Depot”). Plaintiffs bring this Second Amended Consolidated Class Action Complaint against Defendants (f) through (n) (collectively, the “Client Defendants”), individually and as representatives of a defendant class comprised of all other private, non-governmental entities similarly situated to the Client Defendants (hereinafter, “Defendant Class Members”). Plaintiffs complain and allege as follows based on personal knowledge as to

themselves, the investigation of their counsel, and information and belief as to all other matters, and demand a trial by jury.

NATURE OF THE ACTION

1. Without providing any notice and without obtaining any consent, Defendants Clearview, Ton-That and Schwartz (collectively, the “Clearview Defendants”) covertly scraped three billion photographs of facial images from the internet – including facial images of millions of American residents and then used artificial intelligence algorithms to scan the face geometry of each individual depicted in the photographs in order to harvest the individuals’ unique biometric identifiers¹ and corresponding biometric information² (collectively, “Biometrics”). Further, the Clearview Defendants created a searchable biometric database (the “Biometric Database”) that contained the above-described Biometrics and allowed users of the Biometric Database to identify unknown individuals merely by uploading a photograph to the database.

2. The Clearview Defendants did not develop their technology out of a desire for a safer society. Rather, they developed their technology to invade the privacy of the American public for their own profit.

3. While the Clearview Defendants have touted their actions and the Biometric Database as being helpful to law enforcement and other government agencies, the Clearview Defendants have made their Biometric Database available to public and private entities and persons, alike. What the Clearview Defendants’ technology really offers is a massive surveillance state. Anyone utilizing the technology could determine the identities of people as they walk down the street, attend a political rally or enjoy time in public with their families. One of Clearview’s

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

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

financial backers has conceded that Clearview may be laying the groundwork for a “dystopian future.”

4. Accordingly, Plaintiffs, on behalf of themselves and similarly situated individuals, bring this action for damages and other legal and equitable remedies resulting from the actions of the Clearview Defendants, the Client Defendants and the Defendant Class Members for their unlawful creation and/or use of the Biometric Database consisting of the Biometrics of millions of American residents, including residents of Illinois, California, New York and Virginia. As alleged below, Defendants’ conduct violated, and continues to violate, Illinois’ Biometric Information Privacy Act (“BIPA”), 740 ILCS 14/1, *et seq.*, as well as other state constitutional, statutory and common laws, causing injury to Plaintiffs and Plaintiff Class Members

PARTIES

5. Plaintiff David Mutnick is, and at relevant times has been, a resident of Illinois, residing in the Northern District of Illinois.

6. Plaintiff Steven Vance is, and at relevant times has been, a resident of Illinois, residing in the Northern District of Illinois.

7. Plaintiff Mario Calderon is, and at relevant times has been, a resident of Illinois, residing in the Northern District of Illinois.

8. Plaintiff Anthony Hall is, and at relevant times has been, a resident of Illinois, residing in the Northern District of Illinois.

9. Plaintiff Isela Carmean is, and at relevant times has been, a resident of Illinois residing in the Northern District of Illinois.

10. Plaintiff Shelby Zelonis Roberson is, and at relevant times has been, a resident of Virginia.

11. Plaintiff Andrea Vestrand is, and at relevant times has been, a resident of California.

12. Plaintiff Aaron Hurvitz is, and at relevant times has been, a resident of New York.

13. Defendant Clearview AI, Inc., formerly known as Smartcheckr Corp., Inc., is a private, for-profit Delaware corporation, headquartered in New York, New York (Defendant and its predecessors, hereinafter “Clearview”). Clearview markets its technology throughout the United States, including in Illinois. Moreover, Clearview obtains the images that underlie its technology from millions of internet-based platforms and websites, including, on information and belief, based on the magnitude of platforms and websites involved, platforms and websites of Illinois companies or companies who operate servers in Illinois. Clearview’s business and unlawful practices extend nationwide, and it has disclosed the Biometrics of unsuspecting individuals to its clients around the country. Clearview continues to engage in this conduct to this day.

14. Defendant Hoan Ton-That is a founder and the Chief Executive Officer of Clearview and an architect of its illegal scheme, as alleged herein. Ton-That’s responsibilities at Clearview included, and continue to include, managing technology matters. At relevant times, Ton-That knew of, participated in, consented to, approved, authorized and directed the wrongful acts alleged in this Second Amended Consolidated Class Action Complaint.

15. Defendant Richard Schwartz is a founder and the President of Clearview and an architect of its illegal scheme. Schwartz’s responsibilities at Clearview included, and continue to include, managing sales. Schwartz knew of, participated in, consented to, approved, authorized, and directed the wrongful acts alleged in this Second Amended Consolidated Class Action Complaint.

16. At relevant times, Defendant Thomas Mulcaire was an attorney licensed in California, Clearview's General Counsel and the Vice President of Defendant Rocky Mountain. Mulcaire provided the Illinois Secretary of State, a Rocky Mountain customer, with his personal information in order to be paid directly for work performed by Rocky Mountain.

17. Defendant Rocky Mountain Data Analytics LLC is a private, for-profit New Mexico limited liability company with its principal place of business in New Mexico. As alleged in more detail below, a unity of interest existed between Rocky Mountain, on the one hand, and Ton-That, Schwartz and Mulcaire on the other that caused the separate personalities of Rocky Mountain and Ton-That, Schwartz and Mulcaire to no longer exist. Further, as alleged in more detail below, Clearview is legally responsible for the actions and conduct of Rocky Mountain. At relevant times, Rocky Mountain solicited business from potential Illinois customers and contracted with the Illinois Secretary of State. Rocky Mountain provided the Illinois Secretary of State with access to the Biometric Database and the Biometrics contained therein.

18. At relevant times, Defendant Macy's, Inc. was a Delaware corporation, that held itself out to as "one of the nation's premier retailers" with approximately 680 department stores and over 100,00 employees. Among the department stores, were stores located in Illinois.

19. At relevant times, Defendant Macy's Retail Holdings, Inc., now known as Macy's Retail Holdings, LLC, was a New York corporation and wholly-owned subsidiary of Macy's, Inc. doing business in Illinois.

20. At relevant times, Defendant Macy's Corporate Services, Inc., now known as Macy's Corporate Services, LLC, was a New York Corporation and wholly-owned subsidiary of Macy's Retail Holdings, Inc. doing business in Illinois. Defendants Macy's, Inc.; Macy's Retail Holdings, Inc., now known as Macy's Retail Holdings, LLC; and Macy's Corporate Services, Inc.,

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.