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

DAVID MUTNICK, for himself and others similarly situated, Plaintiff, v. CLEARVIEW AI, INC., HOAN TON-THAT and RICHARD SCHWARTZ, Defendants.	Case No. _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED** **INJUNCTIVE RELIEF DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff DAVID MUTNICK, on behalf of himself and all other similarly situated individuals ("Plaintiff"), by and through his attorneys, brings this Class Action Complaint against Defendants CLEARVIEW AI, INC., HOAN TON-THAT and RICHARD SCHWARTZ and alleges the following:

INTRODUCTION

1. Almost a century ago, Justice Brandeis recognized that the "greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding."[1] The conduct of Defendant Clearview, as alleged herein, epitomizes the insidious encroachment on an individual's liberty that Justice Brandeis warned about. However, unlike the "men of zeal" described by Justice Brandeis, Defendant Clearview's conduct was not well-meaning. Rather, Defendant Clearview acted out of pure greed.

[1] *Olmstead v. United States*, 277 U.S. 438, 479 (Brandeis, J., dissenting).

2. Without obtaining any consent and without notice, Defendant Clearview used the internet to covertly gather information on millions of American citizens, collecting approximately three billion pictures of them, without any reason to suspect any of them of having done anything wrong, ever. After obtaining these images, Clearview used artificial intelligence algorithms to scan the facial geometry of each individual depicted in the images, a technique that violates multiple privacy laws. Clearview now furnishes this data to law enforcement agencies throughout the United States, including law enforcement agencies in Illinois, for a fee. Much like dossiers that police departments keep on prior suspects and convicted criminals to use in future investigations, these agencies are now using Clearview's database. However, almost none of the citizens in the database has ever been arrested, much less been convicted. Yet these criminal investigatory records are being maintained on them, and provide government almost instantaneous access to almost every aspect of their digital lives.

3. What Defendant Clearview's technology really offers then is a massive surveillance state with files on almost every citizen, despite the presumption of innocence. Indeed, one of Defendant Clearview's financial backers has conceded that Clearview may be laying the groundwork for a "dystopian future." Anyone utilizing the technology could determine the identities of people as they walked down the street, attended a political rally or enjoyed time in public with their families.

4. Moreover, by controlling the database privately, Clearview received, and continues to receive, real-time access to criminal investigations – it knows who the police are interested in and, often, where those people may be. Thus, Clearview is enmeshed in the use of state power against individual American citizens and, further, has the unique opportunity to tip-off and/or extort suspects.

5. Defendant Clearview's technology poses a grave threat to civil liberties. Constitutional limits on the ability of the police to demand identification without reasonable suspicion, for instance, mean little if officers can determine with certainty a person's identity, social connections, and all sorts of other personal details based on the visibility of his face alone.

6. Moreover, while Defendant Clearview developed its technology in conjunction with law enforcement, the technology is not inherently limited to that use. Clearview has gone on to provide its database to private entities including banks and retail loss prevention specialists. Further, Clearview has actively explored utilizing its technology to allow a white supremacist to conduct "extreme opposition research" and has developed ways to implant its technology in wearable glasses that private individuals could use.

7. Defendant Clearview did not develop its technology out of a desire for a safer society. Rather, Clearview developed its technology to invade the privacy of the American public and monetize citizens' rights for its own profit. In fact, Clearview created its database by violating each person's privacy rights, oftentimes stealing their pictures from websites in a process called "scraping," which violate many platforms' and sites' terms of service, and in other ways contrary to the sites' rules and contractual requirements. Thus, while trying to paint itself as a tool of law enforcement, Clearview actually has conspired with law enforcement to break the law, and violated citizens' rights under the U.S. Constitution in multiple ways, including violating the First Amendment, Fourth Amendment, Fourteenth Amendment and the Contracts Clause of Article I, among others.

8. Plaintiff brings claims on behalf of all American citizens in the Clearview database for injunctive relieve to enforce these vital constitutional rights and for damages against

those responsible for this unconstitutional and anti-democratic scheme (the "Constitutional Rights Class").

9. Plaintiff also brings claims on behalf of the citizens of Illinois in the database (the "Illinois Class"). Specifically, Defendant Clearview's business model blatantly violates the privacy protections in the Illinois Biometric Information Privacy Act, 740 ILCS 13/1, *et seq.* ("BIPA"). In so doing, Defendant Clearview and the individually-named defendants unjustly enriched themselves at the expense of millions of unsuspecting individuals, including Illinois residents.

10. Defendant Clearview's practices have injured Plaintiff and class members ("Class Members") by, among other things, unlawfully obtaining their biometric identifiers and information without consent and, subsequently, selling or otherwise profiting from it.

11. Plaintiff and the Illinois Class retain a significant interest in ensuring that their biometric identifiers and information, which remain in Defendant Clearview's possession, are protected from hacks and further unlawful sales and use. Plaintiff therefore seeks to remedy the harms Clearview and the individually-named defendants have already caused, to prevent further damage, and to eliminate the risks to citizens in Illinois and throughout the United States created by Clearview's business misuse of millions of citizen's biometric identifiers and information.

PARTIES

12. Plaintiff DAVID MUTNICK is an Illinois resident residing in the Northern District of Illinois. At relevant times, images of Plaintiff's face appeared on numerous internet-based platforms and websites.

13. Defendant CLEARVIEW AI, 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.

14. Defendant HOAN TON-THOT is a founder of Defendant CLEARVIEW AI, INC. and an architect of its illegal scheme, as alleged herein. RICHARD SCHWARTZ is a principal of CLEARVIEW and an architect of its illegal scheme. These defendants (collectively the "Individual Defendants") are co-conspirators.

JURISDICTION AND VENUE

15. This Court has jurisdiction under 28 U.S.C. § 1331, as this case brings federal constitutional claims pursuant to 42 U.S.C. § 1983. It also has jurisdiction under 28 U.S.C. § 1332(d)(2) (the "Class Action Fairness Act") because sufficient diversity of citizenship exists between the parties in this action, the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, and there are 100 or more members of the Classes. This Court has supplemental jurisdiction over all the state law claims pursuant to 28 U.S.C. § 1367.

16. This Court has personal jurisdiction over Defendant Clearview because Illinois citizens' rights were a target of its conspiracy, it knew that its conspiracy would cause injury here, it markets and contracts to provide its database in Illinois, and it collected and sold the biometric identifiers and information of Illinois citizens in violation of BIPA. Moreover, without authorization, Clearview scraped images of Plaintiff and Class Members that Plaintiff and Class Members created in Illinois, uploaded from Illinois, and managed via their Illinois-based computers and mobile devices. Further, Clearview obtained the images of Plaintiffs and Class

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.