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

In re: Clearview AI, Inc. Consumer Privacy Litigation	Civil Action File No.: 1:21-cv-00135 Judge Sharon Johnson Coleman Magistrate Judge Maria Valdez

PLAINTIFFS' MEMORANDUM OF LAW IN SUPPORT OF MOTION FOR PRELIMINARY INJUNCTION

INTRODUCTION

Without providing notice or receiving consent, Defendants Clearview AI, Inc. ("Clearview"); Hoan Ton-That; and Richard Schwartz (collectively, "Defendants"): (a) scraped billions of photos of people's faces from the internet; (b) harvested the subjects' biometric identifiers and information (collectively, "Biometric Data"); and (c) created a searchable database of that data (the "Biometric Database") which they made available to private entities, friends and law enforcement in order to earn profits. Defendants' conduct violated, and continues to violate, Illinois' Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, *et seq.*, and tramples on Illinois residents' privacy rights. Unchecked, Defendants' conduct will cause Plaintiffs David Mutnick, Mario Calderon, Jennifer Rocio, Anthony Hall and Isela Carmean and Illinois class members to suffer irreparable harm for which there is no adequate remedy at law.

Defendants have tacitly conceded the need for injunctive relief. In response to Plaintiff Mutnick's preliminary injunction motion in his underlying action, Defendants desperately sought to avoid judicial oversight by claiming to have self-reformed. But Defendants have demonstrated that they cannot be trusted. While Defendants have represented that they were cancelling all non-law enforcement customer accounts, a recent patent application reveals Defendants' commercial aspirations. Further, while Defendants contend that Illinois residents can opt out of the Biometric Database, the opt-out process is a ruse that actually forces Illinois residents to consent to Defendants' collection of their Biometric Data. Illinois residents' should not be forced to provide Defendants with the very information Defendants stole in the first instance in order to get out of a database they never consented to being a part of.

Based on Defendants' above-described conduct and a history of lax security practices, Plaintiffs seek to enjoin Defendants from:

(a) Continuing to possess, use and store the unlawfully collected biometric identifiers and biometric information (collectively, "Biometric Data") of Illinois residents;

(b) Collecting, capturing or obtaining Illinois residents' Biometric Data without first providing the notice and obtaining the releases required by Illinois' Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, *et seq.*;

(c) Selling, trading leasing or otherwise profiting from Illinois residents' Biometric Data; and

(d) Distributing, redistributing or disseminating Illinois residents' Biometric Data without obtaining the consent required by BIPA.

Any preliminary injunctive relief should also require Defendants to:

(a) Store, transmit and protect from disclosure all Biometric Data of Illinois residents: (i) using the reasonable standard of care within Defendant Clearview's industry; and (ii) in a manner that is the same as or more protective than the manner in which the Clearview Defendants store, transmit and protect other confidential and sensitive information; and

(b) Develop and publish on Defendant Clearview's website a written policy, made available to the public, that establishes a retention schedule and guidelines for permanently destroying Illinois residents' Biometric Data when the initial purpose for collecting or obtaining such Biometrics has been satisfied or within three years of the Illinois resident's last interaction with the private entity, whichever occurs first.

The collective relief requested in this paragraph is hereinafter referred to as the "Injunctive Relief." Plaintiffs further request the appointment of a Special Master to assist with the implementation of any Injunctive Relief and to verify Defendants' compliance with any injunction order.

BACKGROUND FACTS

The Parties

Plaintiffs are Illinois residents whose faces have appeared on various websites on the internet. *See* Dkt. 29 ¶¶ 43-47. Clearview is a Delaware corporation founded by Ton-That and

Schwartz. *Id.*, ¶¶ 13-15. Defendants have provided the Biometric Database – consisting of over three billion biometrically-scanned and searchable images – to public and private entities.[1]

BIPA

BIPA strictly regulates an individual's biometric identifiers and information. *See* 740 ILCS 14/1, *et seq.* Under BIPA, biometric identifiers include a "scan of . . . face geometry," and biometric information is "any information . . . based on an individual's biometric identifier used to identify an individual." 740 ILCS 14/10.

In enacting BIPA, the Illinois General Assembly recognized that Biometric Data is sensitive and unique because it cannot be changed if compromised:

> Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information . . . . Biometrics . . . 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.

740 ILCS § 14/5(c).

Defendants' Biometric Database

Defendants have scraped over three billion facial images from the internet and scanned the facial geometry – *i.e.*, the Biometric Data – of each individual.[2] Defendants also built a searchable database of the scanned images – the Biometric Database – thereby enabling database users to

[1] Luke O'Brien, *The Far-Right Helped Create the World's Most Powerful Facial Recognition Technology*, HuffPost (Apr. 7, 2020) ("*The Far-Right Helped Create Clearview*"), https://www.huffpost.com/entry/clearview-ai-facial-recognition-alt-right_n_5e7d028bc5b6cb08a92a5c48 (last accessed on Apr. 9, 2021); Ryan Mac, *et al.*, *Clearview's Facial Recognition App Has Been Used by the Justice Department, ICE, Macy's Walmart, and the NBA*, Buzzfeed News (Feb. 27, 2020) ("*Clearview's Facial Recognition App Use"*), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement (last accessed on Apr. 9, 2021).

[2] *The Far-Right Helped Create Clearview, supra.*

instantly identify unknown individuals using nothing more than a photo.[3] Clearview has boasted that it adds 40 to 50 million new images to the Biometric Database each day. Exhibit 1 (10/8/2019 Clearview email).

Ton-That has described the Biometric Database as "a search engine for faces."[4] According to Ton-That, a person with access to the database can upload thereto a face image of an unknown person, and the database will then: (a) match that face with images in the database; and (b) provide the user with information Defendants have amassed about the person.[5] Over 500,000 face searches have been performed by public and private individuals and entities, including: (a) 8,900 by the Illinois Secretary of State; (b) 7,500 by U.S. Customs and Border Patrol; and (c) more than 8,000 by Immigration and Customs Enforcement.[6]

Defendants do not notify individuals that their Biometric Data is contained in the Biometric Database. Dkt. 29 ¶¶ 1, 60. Defendants do not seek Illinois residents' consent to perform biometric scans on their images, *see id.*, other than in connection with forcing a resident to consent in order to nominally "opt out" of the database, as described above and further discussed below.

The Dangers of the Biometric Database

United States Senator Edward J. Markey has highlighted the grave dangers the Biometric Database poses to the public's civil liberties and privacy: "Clearview's product appears to pose particularly chilling privacy risks" and could be "capable of fundamentally dismantling

---

[3] Donie O'Sullivan, *Clearview AI's Founder Hoan Ton-That Speaks Out [Extended Interview]*, CNN Business (Mar. 6, 2020) ("*Clearview's Founder Speaks Out*"), https://www.youtube.com/watch?v=q-1bR3P9RAw (last accessed on Apr. 9, 2021).
[4] Neil Cavuto, *New Facial Recognition Tech 'Loved' by Law Enforcement: Clearview AI CEO*, Fox Business (Feb. 19, 2020) (*"New Facial Recognition Tech"*), https://video.foxbusiness.com/v/6133890195001/#sp=show-clips (last accessed on Apr. 9, 2021).
[5] *Id.*
[6] *Clearview's Facial Recognition App Use, supra*; *see also* Ryan Mac, *et al.*, *Surveillance Nation*, Buzzfeed News (Apr. 6, 2021), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition (last accessed on Apr. 9, 2021).

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.