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' MOTION FOR A RULING THAT THE CLEARVIEW DEFENDANTS' SOURCE CODE DOES NOT CONSTITUTE "HIGHLY CONFIDENTIAL INFORMATION – SOURCE CODE"

Pursuant to § 11 of the Amended Agreed Confidentiality Order (the "Confidentiality Order") (Dkt. 183), Plaintiffs, by interim lead class counsel, respectfully request that the Court enter an Order finding that the source code produced by Defendants Clearview AI, Inc. ("Clearview AI"); Hoan Ton-That; Richard Schwartz; Rocky Mountain Data Analytics LLC; and Thomas Mulcaire (collectively, the "Clearview Defendants") does not constitute "Highly Confidential Information – Source Code." In support of this motion, Plaintiffs state as follows:

INTRODUCTION

Plaintiffs bring this motion to obtain a ruling from the Court that the source code produced by the Clearview Defendants (the "Source Code") does not constitute "Highly Confidential Information – Source Code," despite the Clearview Defendants designating it as such. The Clearview Defendants cannot meet their burden of establishing that the Source Code is, in fact, "Highly Confidential Information – Source Code." Instead, discovery – and the absence of discovery – has revealed that the Clearview Defendants do not require their employees and contractors to sign non-disclosure or non-compete agreements that would ensure the

confidentiality of the Source Code. Indeed, the Clearview Defendants do not even have their engineers who work directly with the Source Code enter into such agreements.

Moreover, the Clearview Defendants have not produced documents, policies or information showing the internal processes in place, if any, to protect the purported confidentiality of the Source Code. For instance, the Clearview Defendants have not produced evidence showing that: (a) only certain employees or contractors can access the Source Code; (b) access to the Source Code is restricted via a password or biometric scan; (c) employees or contractors may not email, print or otherwise transmit portions or the entirety of the Source Code; (d) employees or contractors may not save the Source Code to a remote device, such as a thumb drive or hard drive; or (e) employees or contractors may not transport the Source Code without restriction.

Notwithstanding the Clearview Defendants' failure to produce the above-described evidence, by designating the Source Code as "Highly Confidential Information – Source Code," the Clearview Defendants have imposed severe limitations on Plaintiffs' ability to review and use the Source Code. There is no justification for imposing on Plaintiffs restrictions with respect to the Source Code that the Clearview Defendants do not otherwise impose in the normal course of their business operations. Because the Source Code is not, in fact, "Highly Confidential Information – Source Code," the Court should grant Plaintiffs' motion and rule that the Clearview Defendants have improperly designated the Source Code.

FACTUAL BACKGROUND

The Confidentiality Order Places Severe Restrictions on the Ability to Review and Use "Highly Confidential Information – Source Code."

The Confidentiality Order defines "Highly Confidential Information – Source Code" as:

> computer code and associated comments and revision histories, formulas, engineering specifications or schematics that define or otherwise describe in detail the algorithms or structure of software or hardware designs, disclosure of which to

> another party or non-party would create a substantial risk of serious harm that could not be avoided by less restrictive means.

Dkt. 183 § 2.D.

Section 4 of the Confidentiality Order sets forth numerous restrictions on the ability to review and use information designated as "Highly Confidential Information – Source Code":

First, the requesting party is required to disclose its consulting experts to the producing party before any source code review can take place to allow the producing party the opportunity to object. *See id.* § 4(a).

Second, any source code review can only take place "during normal business hours on business days or at other mutually agreeable times, at an office of the producing party or producing party's counsel or another mutually agreed upon location that is reasonably convenient for the receiving party." *Id.* § 5(a). The party requesting the review must provide at least 10 days' advance notice for the first inspection and at least two days' notice for subsequent inspections. *Id.*

Third, the source code review may only be performed on a computer without internet access or network access to other computers, printers or storage devices. *Id.* § 5(b). The person conducting the review may not "copy, remove or otherwise transfer any portion of the source code onto any recordable media or recordable device." *Id.*

Fourth, the person conducting the review may not bring into the review room any "smartphone, tablet, blackberry, laptop computer, photographic or video recording device, or any other recording media . . . ." *Id.* § 5(c).

Fifth, the party requesting the review must provide at least five business days' notice of any request to have specific software loaded onto the review computer. *Id.*

Sixth, the person conducting the review is limited in the types of notes that can be taken. *Id.*

Seventh, the producing party may monitor the activities of the person conducting the review. *Id.*

Eighth, the party seeking the review is limited in the number of pages of source code that may be printed. *Id.* § 5(h).

Ninth, the party requesting the source code may only receive a copy of the requested pages on paper and may only transport the source code via hand carry or overnight mail. *Id.* § 5(f).

Plaintiffs' Challenge to the Clearview Defendants' Designation of Their Source Code as "Highly Confidential Information – Source Code"

The Clearview Defendants have designated their Source Code as "Highly Confidential Information – Source Code." *See* Dkt. 162 at 1-2.[1] Plaintiffs have challenged that designation, and the Clearview Defendants have failed to sufficiently rebut the challenge.

Plaintiffs' First Motion to Compel

In Plaintiffs' First Motion to Compel, Plaintiffs argued that the Clearview Defendants sought to "avoid their discovery obligations" by claiming that various discovery requests "seek discovery of *proprietary* information." Dkt. 213 at 9 (emphasis in original). Plaintiffs further argued that the Clearview Defendants "ignore that the requests at issue . . . seek information related to *whether any source code is, in fact, proprietary (e.g., the requests seek non-disclosure agreements and access restrictions*)." *Id.* (emphasis added). The Court granted Plaintiffs' motion and ruled that, "[c]onsistent with Plaintiffs' representation [regarding seeking information related to whether the source code is proprietary], the Court compel[s] Defendants to *produce documents sufficient to identify the proprietary (or non-proprietary) nature of Defendants' source code within 60 days of this Order*." Dkt. 237 at 9 (emphasis added).

[1] Citations to docketed entries are to the CM/ECF-stamped page numbers.

The Clearview Defendants Have Not Produced Non-Disclosure Agreements or Other Documents Showing How Access to the Source Code Is Restricted

Notwithstanding the Court's Order on Plaintiffs' First Motion to Compel, based on a review of the Clearview Defendants' document productions, the Clearview Defendants have not produced non-disclosure agreements restricting disclosure of the Source Code. Exhibit 2 (Drury Decl.) ¶ 2. Further, based on a review of the Clearview Defendants' document productions, the Clearview Defendants have not produced documents showing that: (a) only certain employees or contractors can access the Source Code; (b) access to the Source Code is restricted via a password or biometric scan; (c) employees or contractors may not email, print or otherwise transmit portions or the entirety of the Source Code; (d) employees or contractors may not save the Source Code to a remote device, such as a thumb drive or hard drive; or (e) employees or contractors may not transport the Source Code without restriction. *Id.* 2. Nor have the Clearview Defendants produced non-compete agreements that they required their employees and contractors to sign. *Id.* ¶ 2.

The lack of disclosure and access restrictions is not academic. During the course of this litigation, the Clearview Defendants have disclosed various members of their engineering staff who work with the Source Code but who have not signed agreements limiting their ability to disclose or use the Source Code. Specifically, they have disclosed the following individuals and described their knowledge as follows:

- "Terence Liu – Clearview Vice President of Machine Learning: Clearview's machine-learning algorithms";
- "Kyler Amos – Vice President of Engineering: Development and operations of Clearview's search application"; and
- "Scott Fowler, Noah Gitalis and Justin Godesky may have relevant knowledge about the Clearview app from a technical and/or engineering perspective."

Exhibit 2 (Clearview Def. Resp. to Pl. 1st Set of Interrog.) at 7-8; Exhibit 3 (Clearview Def. 8th Supp. Resp. to Pl. 1st St of Interrog.) at 2-3.

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.