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

In re Clearview AI, Inc., Consumer Privacy Litigation,	)	Case No. 21 C 0135
	)	Judge Sharon Johnson Coleman

ORDER

The Court, in its discretion, denies the Illinois class plaintiffs' motion for a preliminary injunction [30].

BACKGROUND

This multi-district litigation involves defendants' alleged violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* ("BIPA"). Specifically, in their consolidated class action complaint, plaintiffs bring numerous claims under BIPA alleging that the Clearview defendants' conduct violated their privacy rights and that defendants' use of their biometric information was without their knowledge and consent. Plaintiffs allege that the Clearview defendants covertly scraped three billion photographs of facial images from the internet 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 identifiers and corresponding biometric information. Further, plaintiffs explain that the Clearview defendants created a searchable database containing biometrics and allowed users of the database to identify unknown individuals merely by uploading a photograph to the database. The database can be searched remotely by licensed users of the Clearview web application.

Since lead class counsel filed *Mutnick v. Clearview AI, Inc.,* Case No. 20-cv-0512, on January 22, 2020 in this district, the Clearview defendants have taken steps to change their business practices in general and also in relation to the Illinois class. These changes include: (1) blocking all photos

that have metadata associating them with a geolocation in Illinois from being included in search results on the Clearview app; (2) blocking login attempts from IP addresses in Illinois to the best of Clearview's ability; and (3) completing technical modifications to Clearview's collection methods to avoid collecting photos of Illinois residents in the future, among other changes. Clearview has also implemented safeguards to secure its data, such as employee cybersecurity training, encryption of the facial vectors it generates, and deployment of anti-intrusion devices.

LEGAL STANDARD

A "preliminary injunction is an exercise of a very far-reaching power, never to be indulged in except in a case clearly demanding it." *Orr v. Shicker*, 953 F.3d 490, 501 (7th Cir. 2020) (citation omitted). A party seeking a preliminary injunction must first demonstrate: (1) the likelihood of success on the merits; (2) there is no adequate remedy at law; and (3) irreparable harm is likely in the absence of a preliminary injunction. *See Winter v. Natural Res. Defense Council, Inc.,* 555 U.S. 7, 22, 129 S.Ct. 365, 172 L.Ed.2d 249 (2008); *Cassell v. Snyders*, 990 F.3d 539, 544-45 (7th Cir. 2021). If the moving party makes this threshold showing, the Court then considers the balance of harms between the parties and the effect on the public interest. *Tully v. Okeson*, 977 F.3d 608, 613 (7th Cir. 2020). The Court has considerable discretion in determining preliminary injunction motions. *Cassell*, 990 F.3d at 545.

DISCUSSION

The Court turns to whether plaintiffs have established that irreparable harm is likely in the absence a preliminary injunction because it is dispositive. Plaintiffs base their irreparable harm argument on what they call the Clearview defendants' "lax security practices" and two past data breaches of Clearview's electronic systems. Plaintiffs further argue that they will be irreparably harmed based on the existence of two off-shore Clearview subsidiaries, which plaintiffs assert may offer Clearview's software to foreign entities. To establish irreparable harm, the mere possibility of

irreparable injury is not enough; rather, plaintiffs must demonstrate that they will likely suffer irreparable harm in the absence of an injunction. *Orr*, 953 F.3d at 501.

The Court first examines plaintiffs' argument concerning Clearview's lax security practices and two data breaches. The two data breaches exposed Clearview's source code, employee information, and client list—not facial images or facial vectors. In support of their irreparable harm argument, plaintiffs cite newspaper articles outlining the general dangers of security threats, such as the 2017 Equifax data breach. Then, without citing evidence in the record, plaintiffs argue that the Clearview defendants do not take security breaches seriously. A February 26, 2020 Daily Beast article in which Clearview stated "unfortunately, data breaches are part of life in the 21st Century," is not sufficient evidence to suggest that Clearview does not take security breaches seriously. Meanwhile, as discussed above, the Clearview defendants have provided evidence of certain safeguards it has implemented to secure its data.

Plaintiffs' general arguments about the possibility of future data breaches and Clearview's lax security practices suggest a mere possibility of irreparable harm, not that they will likely suffer irreparable harm. Although the Court recognizes plaintiffs need not show that harm has already occurred, *Whitaker v. Kenosha Unified Sch. Dist. No. 1 Bd. of Ed.*, 858 F.3d 1034, 1045 (7th Cir. 2017), plaintiffs must present some evidence from which the Court can draw a reasonable inference that they are likely to suffer irreparable harm before final judgment. Instead of presenting evidence, plaintiffs take issue with Clearview's general counsel, Thomas Mulcaire, and his deposition testimony in which his responses about Clearview's security measures lacked precision and where he admitted he was not a cybersecurity expert. Perhaps Mulcaire was not the best Rule 30(b)(6) witness to testify about Clearview's security measures, but his lack of knowledge does not create a reasonable inference that plaintiffs will likely suffer irreparable harm before final judgment. In short, plaintiffs must do more than show that an irreparable harm "could" arise. *Orr*, 953 F.3d at

502. Moreover, the evidence plaintiffs do present, Clearview's filing of a patent application dated August 7, 2020 describing a broad use of its technology, is too attenuated to suggest that plaintiffs will likely suffer irreparable harm before final judgment, especially because the average time between a patent application and approval is approximately twenty-two months.[1]

As to plaintiffs' argument about the offshore subsidiaries in Panama and Singapore, evidence in the record indicates that these subsidiaries currently have no customers and that they were established to potentially transact with Latin American and Asian law-enforcement authorities. Also, Clearview has yet to authorize these subsidiaries to provide its product in the United States. Under these circumstances, plaintiffs' fear of a future injury is too speculative to support plaintiffs' motion for preliminary injunction. *See Michigan v. U.S. Army Corps of Eng'rs*, 667 F.3d 765, 788 (7th Cir. 2011) ("[A] preliminary injunction will not be issued simply to prevent the possibility of some remote future injury.") (citation omitted).

IT IS SO ORDERED.

Date: 6/14/2021

Entered:

SHARON JOHNSON COLEMAN
United States District Judge

[1] uspto.gov/dashboard/patents/pendency.html