# Clearview AI: A Google Search for Faces

Nicola Roberts-Lewis

In 2016, an Australian tech-entrepreneur set out to create "A Google search for faces."[1] Since then, the program, Clearview AI (Clearview) has transformed into a software used by law enforcement and state governments throughout the country to identify people.[2] Armed with a cache of 40 billion photographs scrubbed from the internet, Clearview created a program that can take a photo of an unidentified person at various locales, such as at an ATM robbery or a political protest, process it through the algorithm, and obtain output of other photos of the individual from other locations, such as Venmo accounts or a university's website.[3]

## Brief History of Clearview and the Technology

With just a general idea of how to proceed, Clearview's founders Hoan Ton-That and Richard Schwartz set out by hiring engineers to develop a program to "scrape" websites of pictures of people's faces.[4] Generally, web scraping uses script to extract data from websites.[5] Clearview specifically mined a variety of websites, such as employment sites, news sites, educational sites, and social networks (including Facebook, YouTube, Twitter, Instagram and even Venmo).[6] The results of this scraping allowed Clearview to amass a database of over 40 billion Facial images.[7] After the images were collected, a facial-recognition algorithm was fine-tuned to convert all the faces in the scraped images into mathematical vectors based on facial geometry.[8] When a user, such as law enforcement, uploads a photo to Clearview for identification , the program maps the person's image and compares its vectors to those stored in Clearview's database.[9]

## Who is using Clearview?

Clearview was initially marketed as a tool for law enforcement agencies, and in 2019, State police agencies experienced remarkable success with the program.[10] Clearview hired Republican officials as representatives of Clearview. These representatives approached law enforcement agencies around the country offering free trials and annual licenses for program use.[11] Since then, US agencies, such as Homeland Security and the FBI, have used the program

---

[1] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, NY TIMES (Nov. 2, 2021), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html; *Facial Recognition Firm Faces Possible £17m Privacy Fine*, BBC (Nov. 29, 2021), https://www.bbc.com/news/business-59466803.
[2] Hill, *supra* note 1.
[3] *Id.*
[4] *Id.*
[5] Tsaone Swaabow Thapelo, *SASSCAL WebSAPI: A Web Scraping Application Programming Interface to Support Access to SASSCAL's Weather Data*, 20 DATA SCIENCE JOURNAL 24, 3.
[6] Hill, *supra* note 1.
[7] *Company Overview*, CLEARVIEW AI, https://www.clearview.ai/overview (last visited Dec. 3, 2023).
[8] Hill, *supra* note 1.
[9] *Id.*
[10] Hill, *supra* note 1 (within 20 minutes of using Clearview, Indiana State Police were able to solve a crime based on security footage).
[11] *Id.*

to track individuals captured on footage from the January 6 Capital Insurrection.[12] Additionally, the program has been used by the Ukrainian military to identify both Russian spies trying to infiltrate Ukraine's population and Russian casualties of the war. [13] The program was also used to determine if anti-fascists trespassed an event at which Donald Trump attended.[14]

**Security and Privacy Concerns**

While the program is being marketed as a tool that stops crime, very real threats and issues accompany the program. First, what happens when this technology falls into the wrong hands? It is being licensed to police departments and state police forces throughout the country with no obvious safeguards on the departments use of the application. For example, a man (with a Clearview license) could take a photo of a woman in a bar and just with that information possibly learn where she lives and works.[15] Additionally, Clearview could be used by authoritarian governments to track political enemies. The program can also be used to determine the identify of a woman leaving an abortion clinic with the purposes of doxing her.

Clearview also suffers from problems that plague other facial-recognition AI programs. Clearview's facial recognition is not perfect and people have been wrongfully accused of crimes.[16] A well-known and supportable criticism of facial recognition technology is that it is racially biased.[17] Such biases can occur as a result of program-developer bias or because of racially skewed datasets.[18] Clearview is not immune to these biases.

**Recent Litigation**

In 2020, the American Civil Liberties Union filed suit against Clearview, claiming that the company violated the Illinois Biometric Information Privacy Act (BIPA).[19] BIPA is a groundbreaking law that was passed in 2008 in Illinois. Biometric data includes retina or iris scans, fingerprints, hand scans, facial geometry, DNA, and other unique biological information.[20] In the case of Clearview and facial recognition, the biometric information in the ACLU's case was facial geometry. BIPA only allows private companies to collect biometric data if they:

- Inform the person in writing of what [biometric] data is being collected or stored. . . .
- Inform the person in writing of the specific purpose and length of time the for which the [biometric] data will be collected, stored and used. . . .

---

[12] Fresh Air, *Exposing the Secretive Company At The Forefront Of Facial Recognition Technology*, NPR (Sep. 28, 2023), https://www.npr.org/2023/09/28/1202310781/exposing-the-secretive-company-at-the-forefront-of-facial-recognition-technology.
[13] *Id.*
[14] *Id.*
[15] Kashmir Hill, *Your Face Belongs to Us: A Secretive Startup's Quest to End Privacy as We Know It* (2023).
[16] Fresh Air, *supra* note 12.
[17] Alex Najibi, *Racial Discrimination in Face Recognition Technology*, SCIENCE IN THE NEWS (Oct. 24, 2020), https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.
[18] Nada Hassanin, *Law Professor Explores Racial Bias Implications In Facial Recognition Technology*, UNIVERSITY OF CALGARY (Aug. 23, 2023), https://ucalgary.ca/news/law-professor-explores-racial-bias-implications-facial-recognition-technology.
[19] Settlement Agreement and Release between plaintiff American Civil Liberties Union and Defendant Clearview AI, (May 4, 2022), https://www.aclu.org/sites/default/files/field_document/exhibit_2_signed_settlement_agreement.pdf.
[20] *Biometric Information Privacy Act (BIPA)*, ACLU ILLINOIS, https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa (last visited Dec. 3, 2023).

- Obtain the person's written consent.[21]

The lawsuit concluded in May 2022 when the ACLU and Clearview reached a settlement agreement.[22] The settlement included a ban on Clearview from licensing the program to (1) any private entity or private individuals (with some exceptions in line with Illinois state law) and (2) any government employee not acting in their official capacity. In addition to these licensing bans, Clearview also agreed to remove faces that Clearview had provided to private individuals from its system and for Illinois residents to opt-out of being a part of the program (as in accordance with BIPA).[23]

**Clearview Is Not the Only One**

Clearview is not the company one would expect to be introducing such a powerful and far-reaching program of identification. Instead, we might think that Google or Meta would have developed this program. In fact, according to a past Google chairman, Google had this capability in 2011, but determined not to bring the product to any market, even law enforcement[24] because was too dangerous.[25]

While large tech companies retained this technology but did not use it, other smaller companies than Clearview offer facial recognition services to private entities. For example, Madison Square Garden implemented facial recognition technology at its large-events venues for security purposes. However, almost fulfilling the prophecy of the technology being too dangerous, the owner of Madison Square Garden used the technology to keep out his "enemies," including attorneys employed by companies suing him.[26] Other programs include PimEyes. Similar to other platforms that sanction multiple users, its use is not limited to government agencies. I could upload a picture of my face right now and maybe get images of myself downloaded from PimEyes.[27] As technology advances, more and more programs like this may become available, and they may be made available to private individuals.

---

[21] *Id.*
[22] Settlement Agreement, *supra* note 19.
[23] *Id.*
[24] Fresh Air, *supra* note 12.
[25] *Id.*
[26] *Id.*
[27] *Id.*