Facial recognition firm Clearview AI tells investors it's seeking massive expansion beyond law enforcement

washingtonpost.com/technology/2022/02/16/clearview-expansion-facial-recognition

February 16, 2022

The facial recognition company Clearview AI is telling investors it is on track to have 100 billion facial photos in its database within a year, enough to ensure "almost everyone in the world will be identifiable," according to a financial presentation from December obtained by The Washington Post.

Those images — equivalent to 14 photos for each of the 7 billion people on Earth — would help power a surveillance system that has been used for arrests and criminal investigations by thousands of law enforcement and government agencies around the world.

And the company wants to expand beyond scanning faces for the police, saying in the presentation that it could monitor "gig economy" workers and is researching a number of new technologies that could identify someone based on how they walk, detect their location from a photo or scan their fingerprints from afar.

The 55-page "pitch deck," the contents of which have not been reported previously, reveals surprising details about how the company, whose work already is controversial, is positioning itself for a major expansion, funded in large part by government contracts and the taxpayers the system would be used to monitor.

The document was made for fundraising purposes, and it is unclear how realistic its goals might be. The company said that its "index of faces" has grown from 3 billion images to more than 10 billion since early 2020 and that its data collection system now ingests 1.5 billion images a month.

With $50 million from investors, the company said, it could bulk up its data collection powers to 100 billion photos, build new products, expand its international sales team and pay more toward lobbying government policymakers to "develop favorable regulation."

No federal law regulates how facial recognition should be used, though some cities and states have passed bans or restrictions. The biggest tech giants, including Amazon, Google, IBM and Microsoft, have limited or ended sales of the technology, saying they are worried about its risks or do not want to sell it to the public before Congress has established rules.

In the presentation, Clearview argues that the industry-wide caution is a huge business opportunity. The company included its rivals' logos to note that it has little domestic competition — and that its product is even more comprehensive than systems in use in China, because its "facial database" is connected to "public source metadata" and "social linkage" information.

The presentation, which a recipient shared with The Post, throws a spotlight on the company's ambitions to become one of the world's leading merchants of surveillance technology, even as some lawmakers worry the company poses a dangerous threat to civil liberties and privacy rights.

Clearview has built its database by taking images from social networks and other online sources without the consent of the websites or the people who were photographed. Facebook, Google, Twitter and YouTube have demanded the company stop taking photos from their sites and delete any that were previously taken. Clearview has argued its data collection is protected by the First Amendment.

Facebook, which forbids the automated copying, or "scraping," of data from its platform and has an External Data Misuse team, has banned Clearview's founder, Hoan Ton-That, from its site and has sent the company a cease-and-desist order, but Clearview has refused to provide any information about the extent to which Facebook and Instagram users' photos remain in Clearview's database, an official with Facebook's parent company, Meta, told The Post. The official declined to comment on any steps Meta may be considering in response.

Clearview's cavalier approach to data harvesting has alarmed privacy advocates, its peers in the facial recognition industry and some members of Congress, who this month urged federal agencies to stop working with the company, because its "technology could eliminate public anonymity in the United States." Sens. Ron Wyden (D-Ore.) and Rand Paul (R-Ky.) last year introduced a bill that would block public money from going to Clearview on the basis that its data was "illegitimately obtained."

Clearview is battling a wave of legal action in state and federal courts, including lawsuits in California, Illinois, New York, Vermont and Virginia. New Jersey's attorney general has ordered police not to use it. In Sweden, authorities fined a local police agency for using it last year. The company is also facing a class-action suit in a Canadian federal court, government investigations in Canada, Sweden and the United Kingdom and complaints from privacy groups alleging data protection violations in France, Greece, Italy and the U.K.

The governments of Australia and France have ordered Clearview to delete their citizens' data, saying the company had covertly monetized people's faces for a purpose "outside reasonable expectations." "The indiscriminate scraping of people's facial images, only a fraction of whom would ever be connected with law enforcement investigations, may adversely impact the personal freedoms of all Australians who perceive themselves to be under surveillance," Australia's information and privacy commissioner, Angelene Falk, said in November.

Ton-That told The Post the document was shared with a "small group of individuals who expressed interest in the company." It included proposals, he said, not just for its main facial-search engine but also for other business lines in which facial recognition could be useful, such as identity verification or secure-building access.

He said Clearview's photos have "been collected in a lawful manner" from "millions of different websites" on the public Internet. A person's "public source metadata" and "social linkage information," he added, can be found on the websites that Clearview has linked to their facial photos.

Facial recognition companies have traditionally built algorithms that can be used to search through their clients' photo databases, such as driver's license images or jail mug shots. But Ton-That has argued in testimony to public officials that swiping photos from the Internet has allowed the company to create a powerful crime-fighting tool. "Every photo in the data set is a potential clue that could save a life, provide justice to an innocent victim, prevent a wrongful identification, or exonerate an innocent person," he said Wednesday in a statement to The Post, an echo of similar assertions he has made in public forums.

Clearview, he told The Post, does not intend to "launch a consumer-grade version" of the facial-search engine now used by police, adding that company officials "have not decided" whether to sell the service to commercial buyers.

If Clearview did decide to sell any technology to a nongovernmental buyer, Ton-That said, the company would first tell a federal court in Illinois, where Clearview is defending itself against class-action claims that it violated a state law requiring companies to obtain people's consent before collecting their facial data.

In a court filing Monday, U.S. District Judge Sharon Johnson Coleman, who is presiding over the case, upheld most of the plaintiffs' arguments challenging Clearview's work.

Clearview has dismissed criticism of its data collection and surveillance work by saying it is built exclusively for law enforcement and the public good. In an online "principles" pledge, the company said that it works only with government agencies and that it limits its technology to "lawful investigative processes directed at criminal conduct, or at preventing specific, substantial, and imminent threats to people's lives or physical safety."

But the presentation shows the company has based its "product expansion plan" on boosting corporate sales, from financial services and the gig economy to commercial real estate. On a slide devoted to its "total addressable market," government and defense contracts are shown as a small fraction of potential revenue, with other possible sources including in banking, retail and e-commerce.

Is there anything "they wouldn't sell this mass surveillance for?" asked Jack Poulson, a former Google research scientist who now runs the research advocacy group Tech Inquiry. "If they're selling it for just regular commercial uses, that's just mass surveillance writ large. It's not targeted toward the most extreme cases, as they've pledged in the past."

Clearview said in 2020 that it would stop working with private businesses after a BuzzFeed News report that found the company had offered its tool to stores, banks and other companies, including through 30-day free trials.

In his statement to The Post, Ton-That said: “Our principles reflect the current uses of our technology. If those uses change, the principles will be updated, as needed.”

Clearview clients can upload a photo to look for matches in the company’s face database, with the results often linking to the person’s other accounts across the Web. The company said its “index of faces” is now 11 times larger than the facial databases of “any government or nongovernment entity today.” (Many of the company’s claims in the document, including that one, could not be independently verified.)

Clearview was a little-known start-up until a New York Times report in early 2020, based on internal emails and public records uncovered by researchers, revealed the extent to which local police departments had begun using it to find potential suspects.

The company said it has since grown its client list to more than 3,100 law enforcement agencies in the United States. It has contracts with the Department of Homeland Security, the FBI and the Army.

Clearview has in the past year built up its executive ranks and advisory board with former high-ranking police and government officials. The company also has championed its work in helping to identify wanted criminals, including alleged rioters at the U.S. Capitol on Jan. 6, 2021.

But much of its new pitch to investors centers on its pursuit of the “limitless future applications” of nongovernment work, including in banking, health care, insurance and retail. “Everything in the future, digitally and in real life, will be accessible through your face,” the presentation says.

The company says in the presentation that it is hoping to raise $50 million in a third round of investment, known as a “Series C.” The company raised $30 million in a similar funding round last summer that valued the company at $130 million.

Its relatively modest valuation, tech experts suggest, could be a reflection of the saturated market for facial recognition algorithms, the company’s precarious legal situation or the fact that its biggest selling point, its vast facial-data cache, has been called “illegitimately obtained.”

The company says in the presentation that it could “revolutionize” how workers in the gig economy are screened and that its technology could be used to evaluate people on apps used for dating or finding babysitters, house cleaners or repair contractors.

The presentation includes the logos for a number of companies, including Airbnb, Lyft and Uber. Ton-That said they were “examples of the types of firms that have expressed interest in Clearview’s facial recognition technology for the purposes of consent-based identity verification, since there are a lot of issues with crimes that happen on their platforms.”

Spokespeople at those three companies told The Post they had no plans to work with Clearview and had never expressed interest in a partnership.

Several other companies whose logos Clearview used as examples of potential business partners, including the babysitter service Sittercity, also said they had no plans to pursue any relationship with the company.

Justine Sacco, a spokeswoman with Tinder and OkCupid parent company Match Group, said that the companies have "never worked with Clearview AI and are not in any discussions with them" and that "Clearview is misusing our logo and does not have permission to use it in their materials." An official at another company expressed anger over it being included in Clearview's presentation and said it was considering legal options.

Clearview also says in the presentation that its systems could be used to solve "tough physical security problems" in retail and commercial real estate markets, and it included the logos of retail superstore companies such as Target and Walmart. Those companies did not immediately respond to requests for comment.

The company says in the presentation that it has developed other systems beyond facial recognition, including for recognizing license plates and "movement tracking," and that it is developing or researching a number of other surveillance techniques: camera software to detect guns and drugs; "gait recognition" systems to identify a person based on how they walk; "image to location" systems to pinpoint a person's whereabouts based on a photo's background; and "contactless fingerprint" recognitions systems to scan a person's identity from afar.

The document offers no details on how those systems work, if at all. Ton-That said the technologies "are all for the purpose of public safety, are in various stages of research and development, and have not been commercialized or deployed in any way."

In an open letter last month, Ton-That said the company could "set an example of using the technology, *not in a real-time way*, but in a way that protects human rights, due process, and our freedoms."

But the presentation directly contradicts him by saying the company is building systems for real-time surveillance. Officials are working toward a "real-time alerts" system that companies could use to notify security agents if it spotted "high-risk individuals," one slide notes.

The company is also continuing work on augmented-reality glasses that the U.S. military could use in "dangerous situations," one slide reads. The Air Force in November awarded the company $50,000 to research the technology, federal spending records show. An official with the Air Force Research Laboratory has said the work is a short-term contract to test how well such technology would work.

In a September letter to the U.K. Surveillance Camera Commissioner office, Ton-That defended the use of real-time facial recognition watch lists for "people of interest, missing people, those with outstanding warrants for serious offenses, or for a specific security-related purpose known in advance."

Clearview says in the presentation that its expansion plans would include spending millions of dollars more on data purchases and engineers specializing in data acquisition and that it would build out its teams specializing in commercial, federal and international sales. It says it also wants to create a "developer ecosystem" that would allow other companies to create applications using its data.

The company said that it expects to increase its annual federal revenue to $6 million this year, thanks to active expansions with DHS and the FBI and an "imminent" expansion from the Drug Enforcement Administration, and that it hopes to "increase overall usage" by state and local police agencies by 300 percent.

U.S. Immigration and Customs Enforcement, a DHS agency, signed a one-year contract with Clearview in September that could extend to three years, totaling $1.5 million, federal records show. The FBI signed an $18,000 one-year contract in December; the presentation says it will grow to $2.4 million this year. The DEA declined to comment, and the FBI and ICE did not respond to requests for comment.

The presentation also says Clearview is "achieving rapid international expansion," including signing deals in Panama and Costa Rica and pursuing other business in Mexico, Colombia and Brazil. The company declined to offer further details, and those deals could not be confirmed.

The Clearview document includes overt appeals to American patriotism, and the company has, as is common among some tech companies, argued that its success is imperative to stopping foreign powers from gaining the lead in surveillance technology development. The company calls itself "Made in the USA" and, in several slides, compares itself with companies from China, Russia and Israel by affixing its logo next to an American flag.

But those arguments, Poulson said, should not distract from the company's expanded ambitions — or its appetite for business far beyond the U.S. government's interests.

"They're explicitly trying to leverage the controversy about their company as a way to argue they're prominent," Poulson said. "And they're combining that with a nationalist rhetoric — that the U.S. has to out-surveil China to protect civil liberties. It makes no sense."

Aaron Schaffer contributed to this report.