The world's scariest facial recognition company, explained

vox.com/recode/2020/2/11/21131991/clearview-ai-facial-recognition-database-law-enforcement

Rebecca Heilweil

February 11, 2020

Lawyer and activist Alyona Popova launched legal action against Russia's vast network of live facial recognition cameras, a system that has been compared to Clearview technology.
Kirill Kudryavtsev / AFP via Getty Images

OPEN SOURCED

How would you like it if anyone armed with an iPhone could figure out a slew of information about you, pull up any Facebook or Instagram picture you've ever been in, and see any other image of you that's been posted publicly online?

This scenario appears to be possible thanks to a shady startup called Clearview AI which, as a New York Times investigation earlier this year revealed, has been mining your pictures online to build a vast facial recognition database. At first, Clearview AI maintained that its tool was only meant to be used by law enforcement and a few private companies. But it later became clear that the company has consistently misrepresented both the extent of its work and the breadth of its aspirations. Now the company seems to be reversing its position, again.

This is concerning. Facial recognition is an incredibly powerful tool, and Clearview's tech is trafficking in highly personal information — including, potentially, yours. (If you're a resident of California or the European Union, feel free to request the data Clearview has on you here, but note you'll likely need to send them a copy of government-issued photo ID.)

Reporting from BuzzFeed News showed that the company had a client list that went far beyond law enforcement and included the NBA, Best Buy, and Macy's, though some of these companies distanced themselves from the facial recognition startup. In early May, however, BuzzFeed followed up with a report that Clearview promised to cease all of its contracts with private companies, as well as any Illinois entities, in an attempt to make moot a lawsuit alleging the company had violated the state's powerful biometric privacy law.

Nevertheless, Clearview has also found a new potential source of business: using its facial recognition as a way to assist Covid-19-related contract tracing efforts. That application quickly worried Sen. Edward Markey, who sent a letter to the company's CEO earlier this week demanding more information. And the startup still faces a slew of other lawsuits.

Clearview exaggerated the role its technology has played in assisting law enforcement in their investigations while also telling Recode that it had only arranged contracts for its technology with customers in the United States and Canada. Documents identified by BuzzFeed News indicate that the company also provided the technology to users in Saudi Arabia and the United Arab Emirates, including to clients with ties to those countries' governments.

And, earlier this year, we learned from a New York Times report that Clearview AI's leaders had even offered up its tech for those connected with the company to try, and that one billionaire used the software to identify a man who was dating his daughter.

The controversy surrounding Clearview has since prompted probes from US senators. The very existence of facial recognition technology has always been a source of debate. Law enforcement has been using facial recognition for several years now, and companies, schools, and other organizations are increasingly making use of the AI-powered software. But Clearview's technology represents a frightening step toward an all-powerful system that the world hasn't seen before. The secretive company says it has created a database of more than 3 billion images that have been scraped from all corners of the internet, including social networks like Facebook, Instagram, and YouTube. From just a snapshot or video still, Clearview claims its app lets someone using the tech identify a face and match it with publicly available information about the person, all within just a few seconds.

Meanwhile, OneZero revealed that Clearview AI had also sought to supplement its database of web-scraped photos with mug shots, though it's not clear whether the company was successful.

Do we want to live in a world where this technology exists? Clearview argues that the tech can help track down dangerous people, and its site points to "child molesters, murderers, suspected terrorists." And as the Times reported in February, the company's facial recognition has helped identify child victims in exploitative videos posted to the web. But clearly the tech can be used for a lot more than that.

And critics say facial recognition is way too risky, enabling excessive surveillance and threatening our privacy rights. Another concern is that the technology, broadly, has also been shown to be less accurate on people of color, women, and other minority groups.

Faced with these concerns, the world's biggest tech companies have stepped up and, sent cease-and-desist letters to Clearview that order the company to stop scraping their sites for our data. But it's not clear how much good that will do, or how invested they actually are in protecting our personal information. While some lawsuits against Clearview are also popping up, it's not yet apparent how Clearview could be stopped. That has privacy advocates pointing to the need for a federal law regulating, or even outright banning, facial recognition in the United States.

Facial recognition isn't new. But this huge database of faces is.

So here's how Clearview's tool works. Say you have an image of a person, but you don't know their name. You could input that photo into Clearview's app, and it will turn up any image of the person that it had scraped from the internet, as well as links to websites from which those images came. That could be a good amount of information.

Again, Clearview's database reportedly includes more than 3 billion images taken from around the web. That's much more than what law enforcement agencies typically have access to. The Times reports that the technology will work with images of faces from many different angles, while older facial recognition tools used by police departments might require the subject to be looking straight ahead, like in a mug shot.

That means images from social media posts on platforms like Instagram could pop up — even images that are no longer, but once were, publicly available. And keep in mind: The tool doesn't just surface pictures that you've taken and posted online. It will also turn up any photos posted of you, even those posted without your consent or knowledge.

"Clearview is a search engine for publicly available images," Clearview CEO Hoan Ton-That told Recode in an email. "We do not and cannot index any images that are private or protected, such as those in a private Instagram account. A previously public image may or may not be searchable with Clearview depending on the time it was public and that would depend on the individual case."

Clearview decides who can — and can't — use this tool

More than 600 law enforcement agencies have used Clearview AI in the past year, as have federal agencies like the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS), according to the Times. The FBI would not confirm to Recode that it had used Clearview's tool, instead pointing to its testimony last year about its use of facial recognition more broadly. The DHS has not responded to Recode's request for comment.

Earlier reporting suggested that the tool was offered to a wide variety of companies for security, though Ton-That wouldn't tell Recode which ones. Now, the company seems to be returning to what it had promised all along: that its tool would only be used for law

enforcement purposes. But with the company repeatedly lying and misrepresenting its own work, it's not clear to what degree its most recent commitment should be trusted.

And even its most recent promise to only sell its product for government purposes doesn't address concerns that its facial recognition tool could be abused by countries with terrible human rights records. Ton-That told the Times earlier this year, "If it's a country where it's just governed terribly, or whatever, I don't know if we'd feel comfortable, you know, selling to certain countries."

But as other reporting indicates, the company has felt comfortable selling this technology to clients in countries with concerning records on civil liberties and human rights, and BuzzFeed earlier reported that the technology had been offered to users in Saudi Arabia and the UAE.

Meanwhile, Clearview had claimed to Recode previously that it does not have contracts outside the US and Canada (The Royal Canadian Mounted Police, the national police service in Canada, told Recode that it does not comment on specific investigative tools but that it researches emerging technologies).

The use of this tool by law enforcement alone raises questions, however. Imagine, for instance, the ethical problems at play with a police officer using Clearview to identify a protester. Or, say the facial recognition doesn't work as it should and a false "match" ultimately leads to arresting someone for a crime they didn't commit.

Initially, there was fear that Clearview's technology could one day be made available to just about anyone. *S*uch a development could destroy our expectation of being anonymous in public.

It's not difficult to imagine terrifying uses of this, and we already have a hint, given how associates of Clearview AI have already made use of the tool. But imagine if a nude picture of you was, at some point in time, posted online. With the snap of a phone camera, it's possible that anyone with Clearview could instantaneously find that image. Or imagine you're walking down the street, and someone decides they want to know where you live and whether you had kids. All they might need is the Clearview app.

The scope of Clearview's threat to privacy remains unclear. The Times has reported: "Police officers and Clearview's investors predict that its app will eventually be available to the public." Unsurprisingly, that was different from what Ton-That told Recode.

"Our strict commitment at this time and at all times previously is and has been not to make this tool available to the general public," Ton-That said in an email to Recode. "Our mission is to reduce crime, fraud, and abuse using our powerful new technology. Any abuse of our technology would be in total violation of our mission and values."

There are many good reasons not to trust this company

Clearview's past has raised alarm bells. For one thing, CEO Hoan Ton-That's previous ventures included an app that added Trump's hair onto photos of people, and he's also been linked to a phishing site. At one point, the company tried to sell a database for "extreme opposition research" to Paul Nehlen, a white supremacist and anti-Semite, who was running for Congress at the time, according to the Times. One investor in the company is Peter Thiel, who helped found PayPay and Palantir and has vocally supported President Trump.

The company hasn't been exactly forthright in its advertising claims, either. For instance, BuzzFeed News reporting found two cases in which Clearview claimed a certain law enforcement agency was "using" its product, when in fact the agency had simply received a tip from the company. Clearview also appears to be claiming that hundreds of police departments were working with them when some of those police departments only signed up for a trial, according to BuzzFeed News.

Ton-That told Recode, "Our calculations are based on the number of agencies that are actively using Clearview's technology to help solve crimes."

It's not quite clear how well the tool actually works. According to marketing materials obtained by BuzzFeed News, Clearview claimed to have "accuracy finding a match out of 1 million faces" 98.6 percent of the time. At the same time, Clearview told the New York Times that the tool produces a match up to 75 percent of the time, although we don't know how many of those are "true" matches. Ton-That also told the Times that one difficulty for Clearview's algorithms is that photos scraped from the web were generally at eye-level, which is not at the same angle typically captured by surveillance cameras.

The company had also said that it had checked the accuracy of its tool using a methodology from the American Civil Liberties Union (ACLU), an assertion the organization has pushed strongly back against. The claim has since been removed from Clearview's site, though the company still says that its tool was reviewed and certified by an "independent panel of experts." (Recode asked Clearview who those experts were, but we never heard back.)

Meanwhile, Craig Watson, the director of the National Institute of Standard and Technology's Image group, told Recode that Clearview had not volunteered to participate in its facial recognition vendor testing program, and there were no plans to evaluate its algorithms.

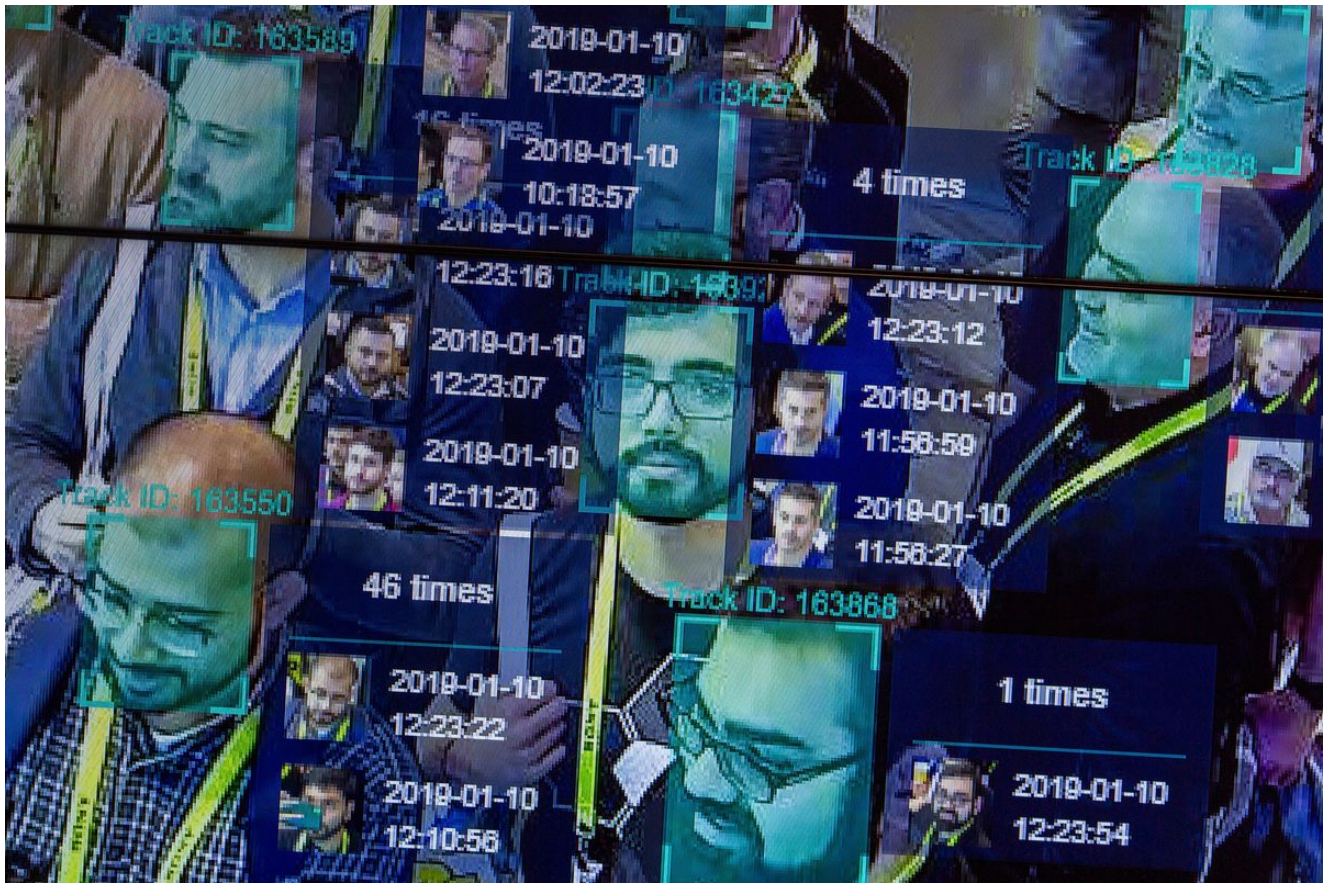
At the same time, Clearview AI also appears to be developing surveillance cameras, according to Buzzfeed News.

Tech companies are fighting back, but that might not be enough

Major internet platforms have responded to Clearview by sending the company cease-and-desist letters. These companies now include LinkedIn, Twitter, Facebook, Venmo, Google, and YouTube. It's worth noting that Twitter explicitly bans using its platform for the purpose of facial recognition. Meanwhile, Pinterest told Recode that it wasn't aware of scraping on its site by Clearview, though such web-scraping would violate their community guidelines. When asked about Clearview scraping its images and videos, PornHub VP Blake White said in a statement, "We have no knowledge of this and actively block scrapers as they violate our Terms of Service."

Apple has since suspended Clearview's access to its developer account for violating its terms.

Still, none of the tech companies that responded to Recode's request for comment have said whether they planned to escalate their demands with lawsuits. Clearview said it has received these letters from companies, and that its "attorneys are responding appropriately." In an interview with CBS, the company's CEO insisted that there is a First Amendment right to public information.



Facial recognition software has become increasingly complex and accurate in recent years. *David McNew/AFP via Getty Images*

As users of these technology platforms, members of the public are now in a curious position. Although we've long criticized these platforms for profiting off our data, we're now potentially reliant on these companies to defend us from a dystopian world of facial recognition. Keep in mind that several of these companies, like Google and Facebook, have worked on facial recognition technology of their own, albeit confronted with varying levels of controversy and ethical concerns. In February, we learned that Facebook had agreed to pay $550 million to settle an Illinois facial recognition lawsuit inspired by its "photo-tagging" suggestion feature. But despite having access to billions of our photos, none of these companies have gone forward with creating such a tool — a boundary Clearview has now crossed.

So Clearview might have your photos. Can you do anything about it?

According to the privacy policy listed on Clearview's site, users have certain rights. But the policy says that the "right to erasure" — deleting your information from their platform — is only available under certain conditions. Although he would not say how many, Ton-That had told Recode that Clearview has received a "number" of these requests and is "responding appropriately."

In a later email, Ton-That said: "We're processing removal requests for persons in jurisdictions that impose that legal requirement." In order to make those requests, you would need to confirm your identity with Clearview by sending in — get this — a photo of yourself on a government ID.

But if you (understandably) don't feel comfortable doing that, you might consider suing Clearview. Several lawsuits have now been filed against Clearview, including in Virginia, Illinois and California. While Texas also has a biometric privacy law, it requires the state's attorney general to take action. That doesn't appear to have happened.

Ton-That said that Clearview designed its tool to follow "all relevant laws and regulation."

Scott Drury, a former Illinois state representative and attorney representing, told Recode back in February that his class action lawsuit was not just arguing that Clearview violated the Illinois Biometric Privacy Act. He said they're also suing on constitutional grounds.

"In this case, you have citizens who clearly have a right to their privacy and they have a right to know how the photographs that they put online are being used," Drury said. "And Clearview, working with law enforcement, specifically and covertly took these photos and scraped them from the internet and didn't let anyone know that they were doing that."

The controversy has prompted some police departments to speak out. Now, the NYPD is denying that it has an "institutional relationship" with the company, according to BuzzFeed News. The Philadelphia Police Department has said that, for now, they're only testing

Clearview AI's tool.

The Chicago Police Department has said that, after a trial, it spent nearly $50,000 to use the tech for two years, according to the Chicago Sun-Times. Meanwhile, the state attorney general of New Jersey has ordered that all police in the state stop using the tool. Others, including the Miami Police Department, have been commenting on cases where Clearview AI has helped to identify suspects.

But a few cities have already banned law enforcement from using facial recognition. The revelations about Clearview AI have also bolstered calls for federal regulation of the technology.

"Congress needs to stop messing around and pass legislation to ban the use of face surveillance technology nationwide," said Evan Greer, the deputy director for the digital rights group Fight for the Future, in a statement. That mimics what other privacy advocates are saying.

And some lawmakers appear to be listening. When the New York Times story came out, Sen. Cory Booker also tweeted that if "Congress doesn't act to limit the use of technology in this manner we risk losing our privacy and our freedom." And at the end of January, Sen. Ed Markey wrote to Ton-That demanding a list of all law enforcement and intelligence agencies in communication with Clearview, along with other questions.

In addition to Markey's newest letter to Clearview AI about contract-tracing, the senator had earlier sent letter directly to the company calling Clearview's initial response "unacceptable," and demanding more information about the company's potential to collect the images of children and its interest in selling its technology to countries with problematic records on human rights.

Still, facial recognition has long been used by law enforcement agencies. So while it's possible that Clearview AI could finally galvanize enough backlash to get lawmakers to act, only time will tell. In the meantime, now would be a great time to switch your social media accounts to private. You friends might care what you were wearing Saturday night, but maybe that's something the cops don't need to know.

Update, March 6: This piece has been since been updated with new details to reflect ongoing reporting on Clearview AI.

Update, May 8: This piece has been updated with new details to reflect ongoing reporting on Clearview AI.

Open Sourced is made possible by the Omidyar Network. All Open Sourced content is editorially independent and produced by our journalists.

Support Vox's explanatory journalism

Every day at Vox, we aim to answer your most important questions and provide you, and our audience around the world, with information that has the power to save lives. Our mission has never been more vital than it is in this moment: to empower you through understanding. Vox's work is reaching more people than ever, but our distinctive brand of explanatory journalism takes resources — particularly during a pandemic and an economic downturn. Your financial contribution will not constitute a donation, but it will enable our staff to continue to offer free articles, videos, and podcasts at the quality and volume that this moment requires. Please consider making a contribution to Vox today.