

Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA

 [buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement](https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement)

The United States' main immigration enforcement agency, the Department of Justice, retailers including Best Buy and Macy's, and a sovereign wealth fund in the United Arab Emirates are among the thousands of government entities and private businesses around the world listed as clients of the controversial facial recognition startup with a database of billions of photos scraped from social media and the web.

The startup, Clearview AI, is facing legal threats from Facebook, Google, and Twitter, as well as calls for regulation and scrutiny in the US. But new documents reviewed by BuzzFeed News reveal that it has already shared or sold its technology to thousands of organizations around the world.

In its quest to create a global biometric identification system to span both public and private sectors, Clearview has signed paid contracts with US Immigration and Customs Enforcement (ICE), the US Attorney's Office for the Southern District of New York, and Macy's, according to the document obtained by BuzzFeed News. The company has credentialed users at the FBI, Customs and Border Protection (CBP), Interpol, and hundreds of local police departments. In doing so, Clearview has taken a flood-the-zone approach to seeking out new clients, providing access not just to organizations, but to individuals within those organizations — sometimes with little or no oversight or awareness from their own management.

Clearview's software, which claims to match photos of persons of interest to online images culled from millions of sites, has been used by people in more than 2,200 law enforcement departments, government agencies, and companies across 27 countries, according to the documents. This data provides the most complete picture to date of who has used the controversial technology and reveals what some observers have previously feared: Clearview AI's facial recognition has been deployed at every level of American society and is making its way around the world.

The New York-based startup has claimed its controversial technology is intended as a tool for police and that it was prioritizing business in North America. "It's strictly for law enforcement," Clearview CEO [Hoan Ton-That said on Fox Business](#) earlier this month. He noted in a Feb. 5 [statement to BuzzFeed News](#) that his company was "focused on doing business in USA and Canada." But in reality, Clearview AI has also been aggressively pursuing clients in industries such as law, retail, banking, and gaming and pushing into international markets in Europe, South America, Asia Pacific, and the Middle East.

Got a tip? Email one of the reporters of this story at Caroline.Haskins@buzzfeed.com or Ryan.Mac@buzzfeed.com, or contact us [here](#).

In reply to an extensive list of questions, Clearview attorney Tor Ekland said, "There are numerous inaccuracies in this illegally obtained information. As there is an ongoing Federal investigation, we have no further comment."

Clearview has attracted a whirlwind of attention for claiming it had built unprecedented facial recognition trained on an ever-increasing database of more than 3 billion photos ripped from Facebook, Instagram, YouTube, and other websites. In a January interview with [the New York Times](#), Ton-That said the company was working with 600 law enforcement agencies across the country and had provided the software, which can be used on a desktop computer or through a mobile app, to the FBI and Department of Homeland Security.

The internal documents, which were uncovered by a source who declined to be named for fear of retribution from the company or the government agencies named in them, detail just how far Clearview has been able to distribute its technology, providing it to people everywhere, from college security departments to attorneys general offices, and in countries from Australia to Saudi Arabia. BuzzFeed News authenticated the logs, which list about 2,900 institutions and include details such as the number of log-ins, the number of searches, and the date of the last search. Some organizations did not have log-ins or did not run searches, according to the documents, and BuzzFeed News is only disclosing the entities that have established at least one account and performed at least one search.

Even with that criteria, the numbers are staggering and illustrate how Clearview AI, a small startup founded three years ago, has been able to get its software to employees at some of the world's most powerful organizations. According to documents reviewed by BuzzFeed News, people associated with 2,228 law enforcement agencies, companies, and institutions have created accounts and collectively performed nearly 500,000 searches — all of them tracked and logged by the company.

While some of these entities have formal contracts with Clearview, many do not. A majority of Clearview's clients are using the tool via free trials, most of which last 30 days. In some cases, when BuzzFeed News reached out to organizations from the documents, officials at a number of those places initially had no idea their employees were using the software or denied ever trying the facial recognition tool. Some of those people later admitted that Clearview accounts did exist within their organizations after follow-up questions from BuzzFeed News led them to query their workers.

“This is completely crazy,” Clare Garvie, a senior associate at the Center on Privacy and Technology at Georgetown Law School, told BuzzFeed News. “Here’s why it’s concerning to me: There is no clear line between who is permitted access to this incredibly powerful and incredibly risky tool and who doesn’t have access. There is not a clear line between law enforcement and non-law enforcement.”

“This is completely crazy. ... There is not a clear line between law enforcement and non-law enforcement.”

There are currently no federal laws regulating the use of facial recognition, though several elected officials have proposed bills. States including Illinois have developed regulations on the corporate use of biometric data, and some cities have outright banned the technology. In that regulatory vacuum, Clearview has thrived, doling out free trials seemingly at will and encouraging law enforcement officers and officials to invite their colleagues and perform as many searches as possible.

On Wednesday, Clearview AI told the Daily Beast that an intruder had “gained unauthorized access to its list” of customers. “Unfortunately, data breaches are part of life in the 21st century. Our servers were never accessed,” Ekeland told the Daily Beast. “We patched the flaw, and continue to work to strengthen our security.”

The explanation did not sit well with some lawmakers, including Oregon Sen. Ron Wyden.

“Shrugging and saying data breaches happen is cold comfort for Americans who could have their information spilled out to hackers without their consent or knowledge,” he told BuzzFeed News. “Companies that scoop up and market vast troves of information, including facial recognition products, should be held accountable if they don’t keep that information safe.”

Clearview CEO Ton-That has been coy about his company’s relationship with the federal government, but documents reviewed by BuzzFeed News suggest his startup has deeply penetrated multiple departments and agencies there. Among them is the Department of Homeland Security, where employees at CBP, the country’s main border security organization, are listed in the documents as having registered nearly 280 accounts. In total, those accounts have run almost 7,500 searches, the most of any federal agency that did not have some type of paid relationship.

A spokesperson for CBP said Clearview was not used for the agency’s biometric entry-exit programs and declined further comment.

Agents at ICE have also used Clearview, according to company documents, running more than 8,000 searches from about 60 different accounts associated with a Homeland Security Investigations field office in El Paso, Texas, an ICE office in Cherry Hill, New Jersey, and a Border Enforcement Security Task Force at New York's John F. Kennedy Airport. The documents also indicate employees of ICE's Enforcement and Removal Operations, the body responsible for the arrest and deportation of those in the country without authorization, have tried Clearview.

A spokesperson for ICE told BuzzFeed News that HSI began a paid pilot program in June 2019 through its Child Exploitation Investigations Unit and noted that a formal contract has not yet been signed.

"ICE's use of facial recognition technology is primarily used by Homeland Security Investigations (HSI) special agents investigating child exploitation and other cybercrime cases," the spokesperson said. "ICE Enforcement and Removal Operations (ERO) officers have also occasionally used the technology, as task force officers with HSI and the Department of Justice, and through training, on human trafficking investigations."

Jacinta González, a senior campaign director at Mijente, a Latinx advocacy group, told BuzzFeed News that ICE's use of Clearview in the absence of a regulatory framework is troubling. "This tool goes way beyond anything that is legal, and there is literally no accountability for how they're going to use this tool," she said. "They could walk into a supermarket, scan people, see if it matches up, and deport them immediately."

Make more work like this possible: Become a [BuzzFeed News member today.](#)

The documents also show that employees at 10 fusion centers, intelligence intake facilities that are recognized by DHS, are deploying Clearview across the country and in the US Virgin Islands. One of those fusion centers in Louisiana was listed as a paying customer.

“They could walk into a supermarket, scan people, see if it matches up, and deport them immediately.”

Clearview has also been used inside the Department of Justice, where the list of government organizations trialing the company's facial recognition software includes multiple offices at the US Secret Service (some 5,600 searches); the Drug Enforcement Administration (about 2,000 searches); the Bureau of Alcohol, Tobacco, Firearms, and Explosives (more than 2,100 searches); and the FBI (5,700 searches across at least 20 different field offices).

Spokespeople for all these agencies either declined comment or did not respond to a request for comment.

Two DOJ organizations — the criminal intelligence branch of the US Marshals and the US Attorney's Office in the Southern District of New York — are paying to use Clearview. A spokesperson for the US Marshals said the organization "cannot confirm the use of any specific, sensitive equipment and techniques that may be deployed by law enforcement," while the US Attorney's Office did not respond to multiple requests for comment.

"Government agents should not be running our faces against a shadily assembled database of billions of our photos in secret and with no safeguards against abuse," Nathan Freed Wessler, a staff attorney with the ACLU, said to BuzzFeed News. "More fundamentally, that so many law and immigration enforcement agencies were hoodwinked into using this error-prone and privacy-invading technology peddled by a company that can't even keep its client list secure further demonstrates why lawmakers must halt use of face recognition technology, as communities nationwide are demanding."

Clearview's technology may have even made it to the White House. Documents reviewed by BuzzFeed News include an entry for "White House Tech Office" with a single user, who logged in back in September 2019 to perform six searches.

The White House did not confirm or deny if that was the case. "If a current or former staff member attempted to access more information about this product, it was not an official inquiry and was not sanctioned by the White House," a senior White House official told BuzzFeed News.

Beyond the federal government, Clearview AI's free trials have inspired facial recognition usage in hundreds of regional, state, county, and local law enforcement agencies. The Miami Police Department, for example, has run over 3,000 Clearview searches, according to the documents. The San Mateo County Sheriff's Office has run about 2,000 searches, as has the Philadelphia Police Department. The Indiana State Police, identified in the startup's documents as a paying agency, has run more than 5,700 scans.

The New York State Police, which has several users who have run dozens of searches, said Clearview is one of many tools used by the agency. The agency paid \$15,000 for Clearview licenses, according to federal spending database GovSpend.

"The Clearview AI facial recognition software is used to generate potential leads in criminal investigations as well as homeland security cases involving a clearly identified public safety issue," a New York State Police representative said to BuzzFeed News.

The bulk of Clearview's paying customers are local and state police departments. The Atlanta Police Department, paid \$6,000 for three licenses last year, according to documents obtained by BuzzFeed News. Officers in Wyomissing, Pennsylvania, paid \$1,000 for a license, according to federal spending database GovSpend.

Clearview AI can be a powerful tool for local police. A representative for the Chicago Police Department — which paid \$49,875 for two-year Clearview log-ins for 30 people — told BuzzFeed News that it is one of two types of facial recognition software the department uses. The first, DataWorks, uses an internal library of mugshots taken in and around the Chicago area. Clearview, meanwhile, employs more than 3 billion pictures from social media and “millions of websites,” according to its CEO, creating a dragnet that could encompass the world. Users with Chicago police, whose contract with Clearview runs through 2021, have collectively run over 1,500 searches.

“If there’s no match [on DataWorks], we try Clearview,” a Chicago police representative said. “DataWorks is a closed system, so it only looks at photos we have. But Clearview uses open source media.”

Jason Ercole, a captain with the Senoia Police Department, which is about 40 miles south of Atlanta, said he started with a free trial of Clearview before converting to a paid license and has since made one positive identification of a suspect who was allegedly cashing fake checks. He said he did not have to go through any training to obtain or use the software and noted he never uses a Clearview match as the sole basis for obtaining a warrant for arrest.

“It’s just like you giving a weapon to a police officer,” Ercole said. “You would hope that he uses it properly and doesn’t use it improperly and remembers his training. It’s a good tool if used appropriately and with caution.”

“It’s just like you giving a weapon to a police officer. You would hope that he uses it properly.”

Clearview’s propensity to hand out free trials to officers using police department or government email addresses has sometimes created situations in which law enforcement agencies appear to have no idea the tool is being used by their employees. While the nation’s largest police department, the NYPD, previously denied it had any formal relationship with Clearview, the document shows that officers there have run more than 11,000 searches, the most of any entity on the document. More than 30 officers have Clearview accounts, according to the logs.

An NYPD spokesperson told BuzzFeed News that while it does not have any contract or agreement with Clearview, its “established practices did not authorize the use of services such as Clearview AI nor did they specifically prohibit it.”

“Technology developments are happening rapidly and law enforcement works to keep up with this technology in real time,” the spokesperson said in a statement. “We are in the process of updating the NYPD’s policy on Facial Recognition practices to address emerging issues.”

Garvie said that these rogue uses of facial recognition are very concerning and that the public has no way of knowing whether all the searches served a law enforcement purpose.

“Not only are these officers operating completely outside of the established outside procedures set up by the NYPD to run these face recognition searches, but they’re vastly expanding the types of cases to which face recognition is actually being applied,” Garvie said.

Even when a police department decides Clearview is not the right fit, it can be hard to prevent officers from using it. The Raleigh Police Department in North Carolina was a paying client but later discontinued its relationship with the startup and put a moratorium on its use of the app after it was unable to get the company to fully comply with an audit.

Despite the severing of that relationship, Raleigh police officers continued to use Clearview beyond the ban on Feb. 11 and signed up with free trials, according to a department spokesperson.

Clearview isn’t only targeting police departments at the state level. Multiple state government agencies are working with the company, according to its logs, including the Illinois secretary of state. Behind the NYPD, it’s run the most searches of any entity on the list, clocking nearly 9,000 scans. A representative for the secretary’s office did not respond to multiple requests for comment.

Clearview’s client list also extends to the American education system, with more than 50 educational institutions across 24 states named in the log. Among them are two high schools.

Those two, Central Montco Technical High School in Pennsylvania and Somerset Berkley Regional High School in Massachusetts, did not respond to a request for comment. Somerset Police Department, which appears on the list with Somerset Berkley Regional, initially denied ever using Clearview or any facial recognition software, but later stated that a detective had received a 30-day free trial. The documents show that each school was only associated with one account. Neither had run more than five searches.

While most universities listed on the documents showed low search counts like the University of Alabama (about 30 searches) or the police at Florida International University (more than 200 searches), the fact that it was being used by officers or officials on campuses at all alarmed activists. In some cases, school officials had no idea it was being used.

“This is exactly why we’ve been calling for administrators to enact a ban,” said Evan Greer, deputy director of Fight for the Future, a digital rights advocacy group. “So much of this happens in secrecy. A security officer shouldn’t be able to use this to stalk students around

campus.”

A spokesperson for New York’s Columbia University, which had one account listed that performed over 30 searches on the list and has similarly committed to not using facial recognition, told BuzzFeed News that “Columbia’s Public Safety has never tested facial recognition technology and there are no plans to use it.” They declined to say why someone associated with the university had tried Clearview.

Southern Methodist University first said that campus police were not using the software, but after multiple follow-ups from BuzzFeed News, a representative admitted that Clearview provided an employee with a test account. “SMU decided not to go forward with it,” an official said, declining to answer further questions about why documents reviewed by BuzzFeed News showed multiple accounts tied to the university.

The University of Minnesota, which had previously committed to not using facial recognition, seemed to have a similar problem after documents showed that employees associated with the campus police department had used Clearview. A university spokesperson told BuzzFeed News that its police department “does not have a contract with Clearview AI.”

“While some individual officers may have been offered trials of the software in the past, use of the program was not and is not part of regular business operations,” said the spokesperson.

More than 200 companies have Clearview accounts, according to the documents, including major stores like Kohl’s and Walmart and banks like Wells Fargo and Bank of America. While some of these entities have formal contracts with Clearview, the majority — as with public sector entities — appear to have only used the facial recognition software on free trials.

Greer said that if people focus conversations about facial recognition only on government or law enforcement uses, they are “missing the bigger picture.”

“The fact that their client list includes all these major corporations shows that private entities can also use this type of invasive technology in incredibly abusive ways,” she said.

For a company that maintains its tools are for law enforcement, Clearview’s client list includes a startling number of private companies in industries like entertainment (Madison Square Garden and Eventbrite), gaming (Las Vegas Sands and Pechanga Resort Casino), sports (the NBA), fitness (Equinox), and even cryptocurrency (Coinbase).

“While we conducted a limited test as we do with an array of potential vendors, we are not and have never been a client of this company,” an NBA spokesperson told BuzzFeed News. A representative for Madison Square Garden told BuzzFeed News after this story’s publication

that the venue demoed the product last year, but didn't move forward with a trial. Clearview's logs show that two accounts associated with the sports and events venue ran more than 70 searches at the end of 2019.

A spokesperson for Coinbase said the company was testing Clearview because of its "unique needs around security and compliance," but it was not using the service with customer data. "Our security and compliance teams tested Clearview AI to see if the service could meaningfully bolster our efforts to protect employees and offices against physical threats and investigate fraud," they said. "At this time, we have not made any commitments to use Clearview AI."

The logs also show the facial recognition startup is particularly interested in banking and finance, with 46 financial institutions trying the tool.

A Bank of America spokesperson confirmed to BuzzFeed News that it's not a paying customer, but declined to explain why Clearview's logs list it as having conducted more than 1,900 searches. "We're not a client of Clearview," a Bank of America spokesperson said. "We haven't been a client, we didn't stop being a client, and we never were a client."

Employees at big-box retailers, supermarkets, pharmacy chains, and department stores have also trialed Clearview. Company logs reviewed by BuzzFeed News include Walmart (nearly 300 searches), Best Buy (more than 200 searches), grocer Albertsons (more than 40 searches), and Rite Aid (about 35 searches). Kohl's, which has run more than 2,000 searches across 11 different accounts, and Macy's, a paying customer that has completed more than 6,000, are among the private companies with the most searches.

Employees at mobile carriers like AT&T, Verizon, and T-Mobile also appear in the Clearview documents. None of these companies appear to be paying customers, but their employees are listed as having collectively run hundreds of Clearview searches. AT&T, which searched for some 200 people, confirmed to BuzzFeed News that the company did not pay for the service, but declined further comment.

Clearview's code of conduct states that individual users must be "authorized by their employer" to use the tool, but that seems to be more of a guiding principle than an enforceable rule. Clearview's documents show that at Home Depot, five accounts ran nearly 100 searches.

"We don't use Clearview AI," a Home Depot representative told BuzzFeed News when asked for comment. "Curious why you thought we're a client."

Garvie was alarmed by Clearview's application to retail settings, noting that it could lead to the profiling of customers for shoplifting or theft.

“We don’t use Clearview AI. Curious why you thought we’re a client.”

“That to me is a concerning premise because not only is there a complete absence of transparency into who gets suspected of shoplifting, and whether there’s any redress provided to an individual,” she said.

The documents reviewed by BuzzFeed News also indicate that the company has provided its software to private investigators and security firms. Among them is Gavin de Becker and Associates, a private security agency, which appears as a paid Clearview customer with more than 3,600 searches, and SilverSeal, a New York firm that engages in private investigation and surveillance, according to its website. Neither firm responded to requests for comment.

When BuzzFeed News reported earlier this month that Clearview AI had used marketing materials that suggested it was pursuing a “rapid international expansion.” the company was dismissive, noting that it was focused on the US and Canada.

The company’s client list suggests otherwise. It shows that Clearview AI has expanded to at least 26 countries outside the US, engaging national law enforcement agencies, government bodies, and police forces in Australia, Belgium, Brazil, Canada, Denmark, Finland, France, Ireland, India, Italy, Latvia, Lithuania, Malta, the Netherlands, Norway, Portugal, Serbia, Slovenia, Spain, Sweden, Switzerland, and the United Kingdom.

The log also has an entry for Interpol, which ran more than 320 searches. Reached for comment, the worldwide policing agency confirmed that “a small number of officers” in its Crimes Against Children unit had used Clearview’s facial recognition app with a 30-day free trial account. That trial has now ended and “there is no formal relationship between Interpol and Clearview,” the Interpol General Secretariat said in a statement.

It’s unclear how Clearview is vetting potential international clients, particularly in countries with records of human rights violations or authoritarian regimes. In an interview with PBS, Ton-That said Clearview would never sell to countries “adverse to the US,” including China, Iran, and North Korea. Asked by PBS if he would sell to countries where being gay is a crime, he didn’t answer, stating once again that the company’s focus is on the US and Canada.

Clearview, however, has already provided its software to organizations in countries that have laws against LGBTQ individuals, according to its documents. In Saudi Arabia, for example, the documents indicate that Clearview gave access to the Thakaa Center, also known as the AI Center of Advanced Studies, a Riyadh-based research center whose clients include Saudi Arabia’s Ministry of Investment. Thakaa, which did not respond to a request for comment, was given access to the software earlier this month, according to the documents.

In the UAE, which criminalizes homosexuality, the company's logs show that Clearview has provided its software to two entities, including Mubadala Investment Company, the country's sovereign wealth fund, which has run more than 100 searches. The facial recognition software has also been used by UAE police, according to the documents, which indicate that it's specifically used for the Ministry of Interior's Child Protection Center in Abu Dhabi.

Outside of the US, Clearview's largest market is Canada, where company logs show access to its app has been given to both public and private entities. There are more than 30 law enforcement agencies in the country with access to the software, including the Royal Canadian Mounted Police, which is listed as a paying customer according to the documents, and the Toronto Police Service, which despite being on free trials have run more than 3,400 searches across about 150 accounts.

Just as in the US, some law enforcement agencies around the world seemed unaware that their officers or employees had signed up and used Clearview. The Australian Federal Police said in a statement that it does not use it but declined to comment on why Clearview's records show that employees associated with the organization have run more than 100 searches — some as recently as January 2020. In the UK, London's Metropolitan Police only told BuzzFeed News that Clearview was not being used in its recently deployed live facial recognition tool but declined to comment on the more than 170 searches noted in Clearview's logs.

Some responses were more ominous. In India, the only entity that has signed up for the software was the Vadodara City Police in the western state of Gujarat. The startup's records show that the department signed up last month and had only run a handful of searches. When asked by a BuzzFeed News reporter if police in the city were still using the facial recognition technology, Police Commissioner Anupam Singh Gahlaut responded with a short text and did not respond to further questions.

"We have not started yet." ●

Hannah Ryan in Sydney, Emily Ashton in the United Kingdom, and Pranav Dixit in Delhi contributed reporting to this story.