Facial Recognition: What Happens When We’re Tracked Everywhere We Go? - The New York Times

Your Face Is Not Your Own

When a secretive start-up scraped the internet to build a facial-recognition tool, it tested a legal and ethical limit — and blew the future of privacy in America wide open.

By Kashmir Hill

Art by Zach Lieberman

In May 2019, an agent at the Department of Homeland Security received a trove of unsettling images. Found by Yahoo in a Syrian user's account, the photos seemed to document the sexual abuse of a young girl. One showed a man with his head reclined on a pillow, gazing directly at the camera. The man appeared to be white, with brown hair and a goatee, but it was hard to really make him out; the photo was grainy, the angle a bit oblique. The agent sent the man's face to child-crime investigators around the country in the hope that someone might recognize him.

When an investigator in New York saw the request, she ran the face through an unusual new facial-recognition app she had just started using, called Clearview AI. The team behind it had scraped the public web — social media, employment sites, YouTube, Venmo — to create a database with three billion images of people, along with links to the webpages from which the photos had come. This dwarfed the databases of other such products for law enforcement, which drew only on official photography like mug shots, driver's licenses and passport pictures; with Clearview, it was effortless to go from a face to a Facebook account.

Listen to This Article

To hear more audio stories from publishers like The New York Times, download Audm for iPhone or Android.

The app turned up an odd hit: an Instagram photo of a heavily muscled Asian man and a female fitness model, posing on a red carpet at a bodybuilding expo in Las Vegas. The suspect was neither Asian nor a woman. But upon closer inspection, you could see a white man in the background, at the edge of the photo's frame, standing behind the counter of a booth for a workout-supplements company. That was the match. On Instagram, his face would appear about half as big as your fingernail. The federal agent was astounded.

The agent contacted the supplements company and obtained the booth worker's name: Andres Rafael Viola, who turned out to be an Argentine citizen living in Las Vegas. Another investigator found Viola's Facebook account. His profile was public; browsing it, the investigator found photos of a room that matched one from the images, as well as pictures of the victim, a 7-year-old. Law-enforcement officers arrested Viola in June 2019. He later pleaded guilty to sexually assaulting a child and producing images of the abuse and was sentenced to 35 years in prison. (Viola's lawyer did not respond to multiple requests for comment.)

At the time, the use of Clearview in Viola's case was not made public; I learned about it recently, through court documents, interviews with law-enforcement officials and a promotional PowerPoint presentation that Clearview made. The case represented the technology's first use on a child-exploitation case by Homeland Security Investigations, or H.S.I., which is the investigative arm of Immigrations and Customs Enforcement. (Such crimes fall under the agency because, pre-internet, so much abuse material was being sent by mail internationally.) "It was an interesting first foray into our Clearview experience," said Erin Burke, chief of H.S.I.'s Child Exploitation Investigations Unit. "There was no way we would have found that guy."

[Read takeaways from this piece: what we learned about Clearview AI and its secret "co-founder."]

Few outside law enforcement knew of Clearview's existence back then. That was by design: The government often avoids tipping off would-be criminals to cutting-edge investigative techniques, and Clearview's founders worried about the reaction to their product. Helping to catch sex abusers was clearly a worthy cause, but the company's method of doing so — hoovering up the personal photos of millions of Americans — was unprecedented and shocking. Indeed, when the public found out about Clearview last year, in a New York Times article I wrote, an immense backlash ensued.

Facebook, LinkedIn, Venmo and Google sent cease-and-desist letters to the company, accusing it of violating their terms of service and demanding, to no avail, that it stop using their photos. BuzzFeed published a leaked list of Clearview users, which included not just law enforcement but major private organizations including Bank of America and the N.B.A. (Each says it only tested the technology and was never a client.) I discovered that the company had made the app available to investors, potential investors and business partners, including a billionaire who used it to identify his daughter's date when the couple unexpectedly walked into a restaurant where he was dining.

Computers once performed facial recognition rather imprecisely, by identifying people's facial features and measuring the distances among them — a crude method that did not reliably result in matches. But recently, the technology has improved significantly, because of advances in artificial intelligence. A.I. software can analyze countless photos of people's faces and learn to make impressive predictions about which images are of the same person; the more faces it inspects, the better it gets. Clearview is deploying this approach using billions of photos from the public internet. By testing legal and ethical limits around the collection and use of those images, it has become the front-runner in the field.

After Clearview's activities came to light, Senator Ed Markey of Massachusetts wrote to the company asking that it reveal its law-enforcement customers and give Americans a way to delete themselves from Clearview's database. Officials in Canada, Britain, Australia and the European Union investigated the company. There were bans on police use of facial recognition in parts of the United States, including Boston and Minneapolis, and state legislatures imposed restrictions on it, with Washington and Massachusetts declaring that a judge must sign off before the police run a search.

In Illinois and Texas, companies already had to obtain consent from residents to use their "faceprint," the unique pattern of their face, and after the

Clearview revelations, Senators Bernie Sanders and Jeff Merkley proposed a version of Illinois’s law for the whole country. California has a privacy law giving citizens control over how their data is used, and some of the state’s residents invoked that provision to get Clearview to stop using their photos. (In March, California activists filed a lawsuit in state court.) Perhaps most significant, 10 class-action complaints were filed against Clearview around the United States for invasion of privacy, along with lawsuits from the A.C.L.U. and Vermont’s attorney general. “This is a company that got way out over its skis in an attempt to be the first with this business model,” Nathan Freed Wessler, one of the A.C.L.U. lawyers who filed the organization’s lawsuit, in Illinois state court, told me.

It seemed entirely possible that Clearview AI would be sued, legislated or shamed out of existence. But that didn’t happen. With no federal law prohibiting or even regulating the use of facial recognition, Clearview did not, for the most part, change its practices. Nor did it implode. While it shut down private companies’ accounts, it continued to acquire government customers. Clearview’s most effective sales tool, at first, was a free trial it offered to anyone with a law-enforcement-affiliated email address, along with a low, low price: You could access Clearview AI for as little as $2,000 per year. Most comparable vendors — whose products are not even as extensive — charged six figures. The company later hired a seasoned sales director who raised the price. “Our growth rate is crazy,” Hoan Ton-That, Clearview’s chief executive, said.

Clearview has now raised $17 million and, according to PitchBook, is valued at nearly $109 million. As of January 2020, it had been used by at least 600 law-enforcement agencies; the company says it is now up to 3,100. The Army and the Air Force are customers. ICE signed a $224,000 deal in August; Erin Burke, of the Child Exploitation Investigations Unit, said she now supervises the deployment of Clearview AI for a variety of criminal investigations at H.S.I., not just child-exploitation cases. “It has revolutionized how we are able to identify and rescue children,” Burke told me. “It’s only going to get better, the more images that Clearview is able to scrape.”

The legal threats to Clearview have begun to move through the courts, and Clearview is preparing a powerful response, invoking the First Amendment. Many civil-liberties advocates fear the company will prevail, and they are aghast at the potential consequences. One major concern is that facial-recognition technology might be too flawed for law enforcement to rely on. A federal agency called the National Institute of Standards and Technology (NIST) periodically tests the accuracy of facial-recognition algorithms voluntarily submitted by vendors; Clearview hasn’t participated. In 2019, the agency found that many algorithms were less accurate in identifying people of color, meaning their use could worsen systemic bias in the criminal-justice system. In the last year, three cases have been unearthed (none involving Clearview) in which police officers arrested and briefly jailed the wrong person based on a bad facial-recognition match. All three of the wrongfully arrested were Black men.

There’s also a broader reason that critics fear a court decision favoring Clearview: It could let companies track us as pervasively in the real world as they already do online.

A majority of us, members of some religious groups excepted and pandemic notwithstanding, go around showing our faces all the time. We post selfies on the internet. Walking down the street, we are unwittingly photographed by surveillance cameras and — as happened to Andres Rafael Viola — by strangers we inadvertently photo-bomb. Until recently, we've had little reason to think deeply about the fact that each of our faces is as unique as a fingerprint or a Social Security number.

Behind the scenes, though, a quiet revolution has been afoot to unlock the secrets of our faceprints. It has been powered by an enormous influx of A.I. expertise into Silicon Valley in recent decades, much of it drawn out of the computer-science departments of elite universities. These experts have been put to work on a number of long-term projects, including language translation and self-driving cars, and one particularly intense area of research has been facial recognition. By 2010, this effort was far enough along for Facebook to introduce a feature called “tag suggestions” that suggested the names of friends who appeared in photos uploaded to its platform. Similar features began proliferating in consumer technology: You could unlock your smartphone by looking at it and then sort all the photos on the device by face. Google’s Nest camera could tell you which neighbor was at the door.

As technology advanced, policymakers didn’t keep up. In the absence of robust regulations, the only thing that kept companies like Facebook and Google from going beyond those basic features we’d grown accustomed to was their own restraint. Deploying facial recognition to identify strangers had generally been seen as taboo, a dangerous technological superpower that the world wasn’t ready for. It could help a creep ID you at a bar or let a stranger eavesdrop on a sensitive conversation and know the identities of those talking. It could galvanize countless name-and-shame campaigns, allow the police to identify protesters and generally eliminate the comfort that comes from being anonymous as you move through the world.

Companies like Facebook and Google forbid “scraping,” or the automated copying of data from their sites, in their terms of service. Still, by encouraging billions of people to post photos of themselves online alongside their names, tech companies provided the ingredients for such a product to succeed, were anyone audacious enough to violate the platforms’ boilerplate legalese. In artificial intelligence, the more data you have, the better your product usually is. It was precisely because of Clearview’s brazen collection of images from popular platforms that it was able to become its industry’s leader.

The main federal law discouraging Clearview from doing that is the Computer Fraud and Abuse Act, passed by Congress in 1986, which forbids “unauthorized access” to a computer. The law was intended to prevent hacking, but some prosecutors have interpreted it as forbidding the violation of a site's terms of service, including by scraping. Clearview's executives, like many entrepreneurs who have come before them, built a company around the gamble that the rules would successfully be bent in their favor.

Their bet was partly validated in the fall of 2019, when a federal judge in the Ninth Circuit ruled in a high-profile case — which LinkedIn had filed against a start-up that was scraping its users' profiles — that automated online copying of publicly available information does not violate the anti-hacking law. The Electronic Frontier Foundation, a civil-liberties group, called the ruling "a major win for research and innovation," because it meant journalists, academics and researchers could automatically collect information from websites without fear. But it was also an excellent precedent for Clearview and its growing database of publicly available photos. (The E.F.F. has since called for federal protections to prevent biometric identification like what Clearview sells.)

The biggest remaining legal hurdle for the company, absent some sudden congressional action, is Illinois's Biometric Information Privacy Act (BIPA), a state law from 2008 that offers the strongest protection in the country for people's faces. The law says that private entities must receive individuals' consent to use their biometrics — a fancy word for measurements taken of the human body — or incur fines of up to $5,000 per use. In 2015, five years after introducing its facial-recognition-based photo tagging, Facebook was hit with a class-action lawsuit in Illinois for violating the law. It settled the suit last year for $650 million.

Clearview is now fighting 11 lawsuits in the state, including the one filed by the A.C.L.U. in state court. In response to the challenges, Clearview quickly removed any photos it determined came from Illinois, based on geographical information embedded in the files it scraped — but if that seemed on the surface like a capitulation, it wasn't.

It could galvanize countless name-and-shame campaigns, allow the police to identify protesters and generally eliminate the comfort that comes from being anonymous.

When I started reporting on Clearview AI in November 2019, the company avoided me. For more than a month, its employees and investors mostly ignored my emails and phone calls. Clearview's then-sparse website listed a company address just a few blocks away from the Times Building in Midtown Manhattan, so I walked over to knock on its door — only to discover there was no building with that address. (The company later told me it was a typo.) I had trouble even finding out who was behind Clearview. Once the company realized I was not going away, it hired Lisa Linden, a seasoned crisis-communications expert, to help deal with me.

In January 2020, Linden introduced me to Hoan Ton-That, Clearview's chief executive, and we met and talked over lattes at a WeWork in New York. Ton-That and I kept in touch. Last March, after I told Clearview I wanted to write about how the company was dealing with the challenges, legal and otherwise, coming its way, he agreed to have phone calls with me every few weeks, under the condition that I not write about them until the publication of this article. In September, Linden invited me to observe a meeting between Ton-That and one of the most accomplished lawyers in the country, Floyd Abrams.

Abrams is a lion of First Amendment law, renowned for defending The New York Times's right to publish the Pentagon Papers 50 years ago. Clearview had hired him, along with a national-security lawyer, Lee Wolosky of Jenner & Block, to defend itself in the Illinois lawsuits. Because of the pandemic, Abrams hadn't been spending much time at the offices of Cahill Gordon & Reindel, the corporate law firm where he is a senior counsel. So on a summery Friday morning, Ton-That met with him instead at Abrams's Fifth Avenue apartment in Manhattan, where visitors are greeted by photos of Abrams shaking hands with Barack Obama and posing with Bill Clinton and George W. Bush.

In his light-filled home office, Abrams — wearing gray slacks, a blue buttonup shirt and a black mask — sat down in a low-slung lounge chair. Six feet away, by the window, was Linden, in a black ensemble and floral-print mask. Ton-That walked in a minute late, dressed in a paisley jacket, a red bandanna functioning as his mask. At 32, Ton-That, who has an Australian mother and claims descent from Vietnamese royalty on his father's side, is tall, slender and elegant. With long black hair and androgynous good looks, he briefly considered a modeling career. He set his gray laptop bag on the floor and reclined in a chair that seemed too small for his lanky body. He came across as serene, without the anxiety you might expect from a person whose company was facing an existential crisis in the courts. He has a performer's ease from years of playing guitar.

Abrams immediately brought up the A.C.L.U. lawsuit in Illinois. The A.C.L.U. said Clearview had violated Illinois's prohibition on using people's faceprints without their consent. Abrams and Ton-That were working on a motion to dismiss the case, arguing that the prohibition violates the company's constitutional right to free speech.

While Floyd Abrams and the A.C.L.U. might not seem like natural enemies — the A.C.L.U. itself being known for defending the First Amendment — Abrams is embracing free speech more radically than the A.C.L.U. is comfortable with, given its concern with civil liberties other than freedom of speech, including individuals' right to privacy. In Abrams's view, Clearview is simply analyzing information in the public realm, an activity the government should not curtail. Abrams's position also reflects a career shift, from primarily defending the constitutional rights of journalists to supporting those of corporations. After the 2008 financial meltdown, he argued that AAA ratings by Standard & Poor's of debt that turned out to be junk were simply the company's opinion and therefore worthy of protection like any citizen's. He represented Mitch McConnell in the 2010 Citizens United case, in which the Supreme Court found that limiting corporations' political spending violated their free speech.

The A.C.L.U. doesn't object to Clearview's scraping of photos, but it says that creating a faceprint from them is "conduct" and not speech — and thus isn't constitutionally protected. Abrams disagrees with that and plans, he said, to argue that analyzing publicly available information (online photos, in this case) and sharing the findings (photos of one particular person) is protected by the First Amendment. Arguing that search results are speech is not without precedent: In 2003, Google won a federal case on similar grounds, after an advertising company accused Google of intentionally lowering its ranking in search results. Clearview had also gathered images from across the web and made them searchable. Google lets you search by name; Clearview lets you search by face.

Abrams saw the Google case as a useful precedent. "We're citing a case that says that a search engine's First Amendment rights would be violated if it were compelled to speak in a manner that the plaintiff wanted," he said to Ton-That. He wanted to write in the motion to dismiss that Clearview's "app makes similar judgments about what information will be most useful to its users."

Then Abrams, who is 84, hesitated: "Is that the way one describes what an app does?" he asked the chief executive. "Does one say the app makes judgments?"

"I wouldn't say we make judgments but provide information," Ton-That said. Then he paused. "Well, I guess we do make judgments in what's similar, but we don't tell them it's a final judgment about who someone is."

"Provides information," Linden suggested.

"On a technical computer level, it's the computer's judgment," Ton-That added. "But we don't want that to be the final judgment when someone is arre- " He stopped himself there.

There is no documented case of Clearview's use resulting in the misidentification of a criminal suspect, but Ton-That was clearly aware that a bad match is possible. The company says that its algorithm is far superior to anything else on the market — a claim that police officers who have used it attest to — though it hasn't submitted its algorithm to NIST for accuracy testing. (Law-enforcement officers told me they would never arrest someone based on facial recognition alone and that a match is only a clue that should lead to further investigation.)

'The primary goal of free speech ought to be protecting the ability to generate knowledge through mechanical means or any means.'

In Abrams's home office, Ton-That did a demo of Clearview. He signed into the app on Abrams's computer, then searched using a photo of Abrams. Usually results appear instantly, but there was a delay, some kind of technological hiccup. Ton-That laughed nervously. "Maybe this is less dangerous than people think," Abrams quipped. But when Ton-That searched instead for Abrams's son, Dan Abrams, a legal correspondent at ABC News, the app performed beautifully: The screen filled with a grid of photos of the younger Abrams from around the web, with the source of each identified in tiny type under the photo. Ton-That clicked on one of the photos, where he was standing with a woman, then clicked on the woman, which brought up numerous photos of her as well.

Those who support Clearview in its legal wranglings are worried that a loss would stifle innovation. "The primary goal of free speech ought to be protecting the ability to generate knowledge through mechanical means or any means," Jane Bambauer, a law professor at the University of Arizona who wrote an amicus brief in support of Clearview's position, told me.

On the other side are those who believe that a ruling in favor of Clearview's methods could usher in a future in which facial recognition is commonplace. Jameel Jaffer, a former A.C.L.U. lawyer who is now the director of the Knight First Amendment Institute at Columbia University, points out that most people who put their photos online over the last two decades very likely didn’t realize their faceprint could be derived from them. He offered the example of going to a hairdresser who also collects your trimmings and sequences the DNA. “If you don’t think that activity is protected by the First Amendment, you have to ask what about Clearview’s activity is different,” Jaffer said.

The cases against Clearview are still in early stages and will probably take years to play out. The company can continue to operate while they do. If it loses this first battle, Abrams plans to appeal, and to keep appealing as many times as needed. He predicts at least one of the cases will eventually make it to the Supreme Court, a place he has argued 13 times in the past.

In recent cases, the Supreme Court has limited the government’s use of new technologies to track people en masse, ruling that the police need a warrant, for example, to collect data about people’s movement from cellphone companies. But the rights of private entities — whether individuals or companies — have been treated differently. In 2011, the Supreme Court heard a case involving a Vermont law that prohibited the sale of information about the drugs doctors were prescribing. Some companies sued, saying the law was unconstitutional because they had a free-speech right to buy and sell that information. The Supreme Court ruled in favor of the companies.

Clearview and the A.C.L.U. will appear before a judge in April to discuss the motion to dismiss. The fact that Clearview’s database is made up of public photos is the core of Abrams’s defense. “We’re saying that where information is already out, already public,” Abrams said, “that the First Amendment provides enormous protection.”

During the year I've been reporting on Clearview, one mysterious subject has been the exact details of the company's origins. According to Ton-That's version of events, he and a man named Richard J. Schwartz founded Clearview AI together. But the pair always struck me as an odd match. Ton-That moved to San Francisco from Canberra in 2007 at age 19 to chase the tech gold rush, spinning up moderately successful Facebook games and iPhone apps and attending Burning Man, but then eventually decamped for New York in 2016. Schwartz is a grizzled New York politico who worked for Mayor Rudolph W. Giuliani in the '90s, edited the New York Daily News editorial page and did communications consulting. He is 30 years older than Ton-That and seems to come from an entirely different world. So, last year, I asked Ton-That how they met and came to found the company together.

Ton-That said he encountered Schwartz in 2016 at the Manhattan Institute, a conservative think tank, during a book event. He said they talked for an hour and decided to meet again for coffee the following week. That time, they chatted for three hours, including about technology and public policy. “And it went from there,” he said. Schwartz later told me he was intrigued by the idea of joining Ton-That’s “brilliant mind and exceptional technical skills with my experience, relationships and know-how.” When the company was first registered in New York in February 2017, using Schwartz’s apartment on the Upper West Side as its business address, it was called Smartcheckr LLC. The name changed to Clearview AI the following year. Ton-That was vague about what happened in those early years, declining to name others involved beyond Schwartz. In Ton-That’s telling, the company just kind of stumbled into facial recognition.

That story never satisfied me. Clearview is a radical new entrant to the technological scene. It dared to contravene a taboo that Google and Facebook — not generally known for their privacy-respecting ways — saw as exceedingly unwise to cross. For the last year, I have tried to figure out the exact genesis of that iconoclastic development and learned that the company’s origin story is more complex than Ton-That made it out to be.

After I broke the news about Clearview AI, BuzzFeed and The Huffington Post reported that Ton-That and his company had ties to the far right and to a notorious conservative provocateur named Charles Johnson. I heard the same about Johnson from multiple sources. So I emailed him. At first, he was hesitant to talk to me, insisting he would do so only off the record, because he was still frustrated about the last time he talked to a New York Times journalist, when the media columnist David Carr profiled him in 2014.

Back then, Johnson was a 26-year-old blogger who would try to poke holes in big stories that were popular with progressives. When a police officer killed 18-year-old Michael Brown in Ferguson, Mo., Johnson sued unsuccessfully to obtain Brown’s juvenile records and published photos from Brown’s Instagram account that he claimed showed a violent streak. Later, Rolling Stone wrote about a University of Virginia student named Jackie who claimed that she was gang-raped at a fraternity, and Johnson called the story a hoax; after the magazine acknowledged discrepancies in Jackie's story, Johnson posted what he said was her last name, along with photos of her. Rolling Stone later retracted the story altogether. Carr criticized Johnson's attack-dog tactics and noted factual errors, calling Johnson a "troll on steroids," but pointed out that he had gotten some notable scoops and was "not without some talent."

Johnson found his tactics and political leanings suddenly becoming more mainstream during the Trump administration, and he began to accumulate real influence. Forbes reported that he helped the White House vet political appointees.

Johnson says he eventually decided to talk to me on the record because he regrets some of his decisions and the notoriety that has haunted him since. He wanted to correct what he feels are mistaken impressions of him by revealing that he helped start a company whose product is now being used to save children from sexual abuse.

Johnson claims that he met Ton-That in 2016, introduced him to Schwartz and considers himself a third co-founder of Clearview. I was skeptical at first, given Johnson's reputation as a peddler of disinformation. In a statement, Ton-That acknowledged that he met Johnson in 2016 and that Johnson had "introduced people to the company." But he said Johnson was not a founder and never had an operational role. Johnson, however, provided email and legal documents that, along with other sources, strongly support his claims; indeed, the company might not exist without his contributions.

According to Johnson's version of events, which Clearview disputes, it all began in May 2016, when Ton-That emailed Johnson, saying he was an admirer of Johnson's work and asking to join a Slack group that he ran for fans of his right-wing takes. The next month, Johnson visited New York, and Ton-That met him for the first time in person. They hung out for at least 10 hours straight and became fast friends, according to Johnson and associates of Ton-That at the time. The people who knew Ton-That said he had always been contrarian, but it surprised them when he came out as a Trump supporter in early 2016. They worried about his new relationship with Johnson, given his extreme views and associations. Ton-That recently described himself as “confused” at that time in his life. He went on: “People get radicalized into things. It’s crazy to see it. I got sucked in for a while.”

That summer, the new friends attended the Republican National Convention in Cleveland, where Donald Trump was being crowned the party’s presidential nominee. Johnson had rented a big group house on Airbnb. “Am I still allowed to crash?” Ton-That wrote in an email to Johnson, which Johnson provided to me. “I’ll bring my guitar, can chip in for accommodations.”

“Yes, of course,” Johnson replied. “Want to meet Thiel?”

“Of course!” Ton-That wrote back.

“Thiel,” of course, was Peter Thiel, one of the most powerful men in Silicon Valley — though he no longer lives there, having moved to Los Angeles. (A spokesman for Thiel did not respond to requests for comment.) He famously turned an early $500,000 investment in Facebook into a billion dollars and became a founder of Palantir, a data-gathering juggernaut.

Thiel was in Cleveland because he had come out in support of Trump and was giving a prime-time speech at the convention. Johnson sent me a photo taken of him and Ton-That on the floor of the arena: Both men are smiling, with Thiel visible on a screen behind them.

While Johnson and Ton-That hung out at the rental house, they mused about discredited sciences that could be explored in the modern age with new technologies. At one point, the conversation turned to physiognomy, the pseudoscientific judgment of a person’s character based on their facial features. “Hoan played music,” Johnson said. “We all drank a lot.” He added, “That was where a lot of ideas that became Smartcheckr, and then Clearview, began.” Johnson told me he also arranged a meeting between Thiel and Ton-That at a home in Shaker Heights that week.

Johnson says he was the one who brought in Schwartz, because of Schwartz’s deep political connections in New York — including at the N.Y.P.D. — and because he offered an inroad to Trump as a former Giuliani lieutenant. Two days after the convention ended, Johnson emailed Ton-That and Schwartz, introducing them. Within a week, they made plans to meet, according to an email thread that Johnson forwarded to me.

Seven months later, in February 2017, Schwartz emailed draft formation documents for a company called Smartcheckr LLC to Johnson, which granted equal ownership to Schwartz, Ton-That and Johnson. It was a name that would seem to have Johnson’s fingerprints all over it — he previously founded start-ups called WeSearchr and FreeStartr — though the company claims the name was Schwartz’s idea. “I am very excited about our new company and look forward to the great work you, Hoan and I will be doing together!” Schwartz wrote.

Ton-That says the LLC “was not intended for the purpose of developing facial-recognition technology, and it conducted no business.” Johnson claims the plan from the beginning was to make an app to identify faces. In June 2017, Ton-That emailed Schwartz, Johnson and another person a link to a Scientific American article about Caltech researchers who had shed new light on how the brain identifies faces. Schwartz responded, “Sounds like Caltech is a year behind you.”

In July 2017, a director at Thiel Capital, an investment firm founded by Thiel, emailed Ton-That to say that Thiel was interested in investing $200,000. Ton-That forwarded the email to Johnson. Thiel soon did invest.

Johnson was living on the West Coast, dealing with a new child and a disintegrating marriage, and while he was introducing the company to potential funders and clients, he was not involved in day-to-day operations. In August 2017, Smartcheckr registered as a corporation in Delaware. This time, Schwartz and Ton-That were listed as the only directors.

That fall, perhaps trying to keep some money coming in while improving its facial-recognition technology, Smartcheckr pitched itself to political candidates as a consulting firm. A person close to the company in its early days said the founders wanted to dig up dirt on liberals, which the company and Johnson deny. Paul Nehlen, a far-right Republican running for Congress in Wisconsin, publicly claimed the company had sent him a brochure about "enriched" voter profiles, "microtargeting" of voters and "extreme opposition research." (Nehlen didn't respond to requests for comment.) When I asked the company about his claims last year, it told me it never actually offered such services and that the email came from a rogue contractor. But I found out that it was not a one-off — nor was the outreach limited to Republicans.

Schwartz offered the same Smartcheckr services, in October 2017, to a Democratic newcomer to politics named Holly Lynch, a communications consultant who was running for a congressional seat in New York. According to Lynch, he told her he had a great guy who could be very helpful with voter data, called the Prince — a reference to Ton-That's royal ancestry. Lynch said Schwartz didn't mention facial recognition, only "unconventional databases." Lynch ultimately chose not to work with Smartcheckr and soon ended her campaign.

It appears Smartcheckr decided against pursuing political consulting. The facial recognition it had been working on had improved. "It wasn't clear it would work until April 2018, when the accuracy part really kicked in," Ton-That said.

Two months later, the company changed its name to Clearview AI. That summer, it pitched itself as a security start-up and conducted pilot facial-recognition projects with branches of TD Bank and Gristedes Supermarket in

Manhattan, according to a document provided to a potential investor. (Gristedes's owner, John Catsimatidis, confirmed its project; TD Bank said it "does not have a business relationship with Clearview AI and does not use any of Clearview AI's products.") Another investor who was approached by the company said that the product was impressive but that the ties to Charles Johnson scared him off. (He did not want to be named, fearing retribution from Johnson.)

During the course of 2018, Clearview's database grew to a billion faces from 20 million. At the end of the year, the founders dissolved the LLC they formed in New York and asked Johnson to sign a "wind-down and transfer agreement," which converted his one-third ownership in Smartcheckr LLC into a 10 percent stake in Clearview AI. The contract also entitled him to a 10 percent sales commission on any customers he introduced to the company, though Johnson hasn't been paid a commission.

The wind-down agreement, which Johnson provided to me, requires him not to "publicly disclose the existence of this agreement, his indirect ownership of the shares or his prior provision of services to the company." It is signed by Johnson, Ton-That and Schwartz. (In early March, Clearview amended its incorporation documents such that any shareholder who "breaches any confidentiality obligations" can have his or her shares bought back at 20 percent of market value. When I told Johnson about this, he responded, "That's probably not good for me.")

Johnson said in February that he was willing to break the agreement, both because he's upset about having been erased from Clearview's past and because he thinks the company should have gone further than it has in making the technology available. Johnson believes that giving this superpower only to the police is frightening — that it should be offered to anyone who would use it for good. In his mind, a world without strangers would be a friendlier, nicer world, because all people would be accountable for their actions.

“I think Clearview should be in the hands of the moms of America,” he said.

No matter its parentage, Clearview was inevitable. All the building blocks were there; it was just a matter of picking them up and putting them together. But it makes sense that Thiel, who seems to see personal data as a resource to be mined for riches, and Johnson, who made a career of digging up dirt on people, were part of the company’s origins. Our faces are crucial to linking the digital data that’s been accumulated about us with our identities in the real world. That is valuable not just to law enforcement but also to companies, advertisers, journalists and, yes, the moms of America.

The fact that this superpower is not yet available to us all may just be a fluke of history. Suppose it had been Charles Johnson, not Hoan Ton-That, who ended up at the company’s helm. Or suppose — even before Clearview began — that an influential executive at Google or Facebook had successfully pushed for using the photos and algorithms they already had to let people search for faces as easily as we now search for text.

In some countries, facial recognition is already becoming as mainstream as other once-unimaginable technologies now taken for granted. In 2016, a Russian company called NTechLab developed a facial-recognition algorithm used in an app called FindFace, which matched photos of strangers to profiles on VK — essentially Russia's Facebook. Within months of its release, it was reported that people were using the app to identify sex workers, porn stars and protesters. NTechLab shut down the public FindFace app but still provides its algorithm to governments and corporations. In 2019, the technology was placed in Moscow surveillance cameras, providing a live log of who passed the cameras and when. Meant to be used to find criminal suspects, it was repurposed to enforce lockdown during the Covid-19 pandemic. In March, a man who was supposed to be quarantining went outside his apartment to take out the trash; 30 minutes later, the police were at his door.

In China, facial recognition aids in surveilling the population and in enforcing both the law and social norms. In Suzhou, local authorities have deployed it to name and shame people wearing their pajamas in public. Other uses are quite a bit more sinister, including automatically flagging the faces of Uighurs and other ethnic minorities and tracking their comings and goings. In 2018, Chinese police officers began testing out facial-recognition glasses that would let them more easily ID the people they interact with. When The New York Times analyzed a copy of the computer code underlying the Clearview AI app, a data journalist at the paper found that it, too, was designed to be able to run on augmented-reality glasses. (The company says it has experimented with this function only in its lab.)

Facial recognition would of course look different in the American context, where the state's reach is significantly more curtailed — by both laws and norms — than it is in China or Russia. The more society-changing aspect of facial recognition in the United States may be how private companies deploy it: Americans' right to privacy is relatively strong when it comes to the federal government but very weak when it comes to what corporations can do. While Clearview has said it doesn't want to make its app available to the public, a copycat company could. Facebook has already discussed putting facial recognition into augmented-reality glasses. Within the last year, a mysterious new site called PimEyes has popped up with a face search that works surprisingly well.

Retail chains that get their hands on technology like this could try to use it to more effectively blacklist shoplifters, a use Rite Aid has already piloted (but abandoned). In recent years, surveillance companies casually rolled out automated license-plate readers that track cars' locations, which are frequently used to solve crimes; such companies could easily add face reading as a feature. The advertising industry that tracks your every movement online would be able to do so in the real world: That scene from "Minority Report" in which Tom Cruise's character flees through a shopping mall of targeted pop-up ads — "John Anderton, you could use a Guinness right about now!" — could be our future.

The more society-changing aspect of facial recognition in the United States may be how private companies deploy it.

And imagine what you would do with a face-identifying app on your phone: a Shazam for people. You would never forget someone's name at a party again. If that pseudonymous troll on Twitter who said something nasty to you had ever tweeted a selfie, you could find out who he or she was. You could take a photo of the strangers at your poker table and know if they're pros or not. It might just be your new favorite app.

Alvaro Bedoya, a former congressional staff member who started a privacy center at Georgetown Law School, told me widespread facial recognition could both empower the government and transform civilian life — outcomes that he called “equally pernicious.” He thinks, for example, that ICE could start searching out visa overstayers for deportation by using the photos taken when they entered the country and scanning surveillance-camera feeds for them once their documentation expires. And anonymity could be eradicated in day-to-day life.

“When we interact with people on the street, there’s a certain level of respect accorded to strangers,” Bedoya told me. “That’s partly because we don’t know if people are powerful or influential or we could get in trouble for treating them poorly. I don’t know what happens in a world where you see someone in the street and immediately know where they work, where they went to school, if they have a criminal record, what their credit score is. I don’t know how society changes, but I don’t think it changes for the better.”

It’s impossible, of course, to perfectly predict how novel technologies will ultimately be used and how they will reshape our world. On the day the Capitol was stormed by pro-Trump rioters in January, Ton-That was at work in his Chelsea apartment. Then his phone began to buzz with text messages and phone calls from friends and colleagues, predicting that Clearview AI would be critical for identifying participants; despite the pandemic and the seemingly obvious incentives to conceal their identities, most of the rioters’ faces were exposed. One of Ton-That’s salespeople called because a police officer wanted free access. “I said we could because it was an emergency situation,” Ton-That said.

And in fact, the next day, the company saw a surge in searches from law enforcement. The F.B.I. wouldn’t discuss whether Clearview AI was being used for its investigation of the riot, but detectives in Alabama and Florida who collaborate with the bureau at real-time crime centers said they had identified possible rioters using Clearview and sent them to the F.B.I. “We are up to six potential matches,” an assistant Miami Police Department chief, Armando R. Aguilar, told me a week after the riot. The following week, the number was 13.

It was a remarkable turn of events. The relationships behind Clearview had germinated at an event celebrating Trump, at least according to Johnson; now, four years later, the app was being deployed in a domestic crackdown on lawbreaking Trump supporters. There had been a time when public opinion seemed set firmly against facial recognition. But suddenly — with people showing their faces while rampaging through the Capitol — Clearview and similar products seemed quite appealing.

Ton-That and I talked on the phone just a couple of days after the riot. He sounded tired and spoke hurriedly — he was pressed for time, he said, because of the incoming demand from law enforcement. He didn't seem to harbor any remaining allegiance to Trump, calling the attack "tragic and appalling" and declaring that the transition of power should be peaceful. While he was clearly taken aback by the events unfolding in his adopted country, he also seemed keenly aware it could demonstrate the utility of his company's product, and perhaps sway those on the fence if it played a role in finding and punishing the people involved.

"You see a lot of detractors change their mind for a somewhat different use case," he said. "We're slowly winning people over."

Kashmir Hill is an investigative reporter for the business section of The New York Times. She writes about the unexpected and sometimes ominous ways technology is changing our lives, particularly when it comes to our privacy.

Video by Malike Sidibe and Owen Dubeck for The New York Times.

Hair and makeup: Markphong Tram.

Additional design and development by Jacky Myint.